The Dissertation Committee for John Matthew Garza

certifies that this is the approved version of the following dissertation:

The Height in Terms of the Normalizer of a Stabilizer

Committee:

Jeffrey Vaaler, Supervisor

John Tate

Clayton Petsche

Fernando Rodriguez-Villegas

Felipe Voloch

The Height in Terms of the Normalizer of a Stabilizer

by

John Matthew Garza, B.S.

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

May 2008

The Height in Terms of the Normalizer of a Stabilizer

Publication No. _____

John Matthew Garza, Ph.D.

The University of Texas at Austin, 2008

Supervisor: Jeffrey Vaaler

This dissertation is about the Weil height of algebraic numbers and the Mahler measure of polynomials in one variable. We investigate connections between the normalizer of a stabilizer and lower bounds for the Weil height of algebraic numbers. In the archimedean case we extend a result of Schinzel [Sch73] and in the non-archimedean case we establish a result related to work of Amoroso and Dvornicich [Am00a]. We establish that amongst all polynomials in $\mathbb{Z}[x]$ whose splitting fields are contained in dihedral Galois extensions of the rationals, $x^3 - x - 1$, attains the lowest Mahler measure different from 1.

Contents

Chapter 1 Absolute Values **1**

1.1 Definition 1

1.2 Completions 4

1.3 Absolute Values on the Rational Numbers 8

1.4 Valuations 9

1.5 The Places of an Algebraic Number Field 11

1.6 The Galois Action on Places 15

1.7 Ideals and Valuations of Algebraic Number Fields 16

1.8 Decomposition Groups of Prime Ideals in $\mathcal{O}_{\mathbb{K}}$ 19

1.9 The Stabilizer of a non-Archimedean Place of $\mathbb{K}$ 22

Chapter 2 The Absolute Weil Height **27**

2.1 Definition 27

2.2 Elementary Properties 29

2.3 Lower Bounds for the Height 35

2.4 The Height of Complex Conjugation 40

2.5 Non-Archimedean Estimates 48

2.6 An Example 66

Chapter 3 The Mahler Measure **69**

3.1 Definition 69

3.2 Lehmer's Problem 74

3.3 Reciprocal Polynomials 75

3.4 Lengths, Discriminants and Derivatives 76

3.5 Unconditional Lower Bounds 80

3.6 Bounds Based on Algebraic Properties 81

3.7 Extremal Polynomials 82

Chapter 4 Dihedral Extensions **85**

4.1 Introduction 85

4.2 Orders not Divisible by 4 86

4.3 Subgroups of Dihedral Groups 89

4.4 The Subgroup $H_{\mathbb{Q}(\alpha)} \leq \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ 96

4.5 Estimates for $A \equiv \prod_{v \mid \infty} a_v^{(d_v/d)}$ 98

4.6 Numbers of Degree ≥ 10 102

4.7 Numbers of Degree ≤ 8 119

4.8 Final Remarks 146

Bibliography **148**

Vita **152**

Chapter 1

Absolute Values

1.1 Definition

An *absolute value* on a field k is a map $|\cdot| \ : \ k \ \longrightarrow \mathbb{R}^+ \bigcup \{ \ 0 \ \}$ that satisfies the following three properties

$$\begin{aligned} (i) \quad |x| &= 0 \quad \text{if and only if} \ \ x = 0 \\ (ii) \quad |x \cdot y| &= |x| \cdot |y| \ \ \text{for all} \ \ x, \ y \ \in k \\ (iii) \quad |x + y| &\leq |x| + |y| \ \text{for all} \ x, \ y \ \in k \end{aligned}$$

The absolute value $|\cdot|_0$ on k defined by

$$|x|_0 = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$$

is called the *trivial* absolute value on k. Any other absolute value on k is said to be *nontrivial* and from now on we will assume that all absolute values under

consideration are nontrivial.

If $|\cdot|$ is an absolute value on k then $|\cdot|$ is a group homomorphism from $(k^\times, \times)$ to $(\mathbb{R}^+, \times)$. It follows that $|1| = 1$ and more generally that for a root of unity ζ, $|\zeta| = 1$. We also have that for all $x \in k^\times$, $|x^{-1}| = |x|^{-1}$.

Let M_k denote the set of all absolute values on k. If $|\cdot| \in \mathrm{M}_k$ then the map $(x, y) \longrightarrow |x - y|$ from $k \times k$ to $[0, \infty)$ is a metric and therefore induces a metric topology on k. We say that two elements of M_k are *equivalent* if they induce the same metric topology on k. This defines an equivalence relation on M_k and we call an equivalence class of M_k a *place of* k. In this thesis $\mathcal{A}_k$ will denote the set of places of k.

An absolute value, $|\cdot|$, is said to be *non-archimedean* if for all x and $y \in k$

$$\Big| x + y \Big| \leq \max\Big\{ |x| , |y| \Big\} \tag{1.1.1}$$

in which case inequality (1.1.1) is called the *ultrametric* or *strong triangle inequality*. If there exists x and $y \in k$ such that $|x + y| > \max\{ |x| , |y| \}$ then the absolute value is said to be *archimedean*. If an absolute value is archimedean then all other absolute values in the same place are archimedean and we can describe the places of k as being archimedean or non-archimedean. An archimedean place will also be called an *infinite place* while a non-archimedean place will also be called a *finite place*. Equivalent absolute values are characterized by the following theorem which can be deduced from Section 4.1 of [Koc00].

Theorem 1.1.1. (Other Characterizations of Equivalence) *Let* $|\cdot|_1$ *and* $|\cdot|_2$ *be absolute values on* k. *Then the following are equivalent:*

(1) $|\cdot|_1$ and $|\cdot|_2$ induce the same metric topology on k,

(2) $\{\ x\ \in\ k :\ |x|_1 < 1\ \}\ =\ \{\ x\ \in\ k\ :\ |x|_2 < 1\ \}$

(3) there exists a positive number θ such that $|x|_1^{\theta} = |x|_2$ for all $x \in k$.

Let $|\cdot|$ be a nontrivial and non-archimedean absolute value on k. For $N \in \mathbb{N},\ N \geq 2$, let $\alpha_1,\ \ldots,\ \alpha_N\ \in\ k$ be such that $|\alpha_N| > |\alpha_i|$ for $1 \leq i < N$ then

$$\begin{aligned}
\Big|\ \alpha_N\ \Big| &= \left|\ \sum_{i=1}^{N} \alpha_i - \sum_{i=1}^{N-1} \alpha_i\ \right| \\
&\leq \max\left\{\ \left|\ \sum_{i=1}^{N} \alpha_i\ \right|,\ |\alpha_1|,\ \ldots,\ |\alpha_{N-1}|\ \right\} \\
&= \left|\ \sum_{i=1}^{N} \alpha_i\ \right| \\
&\leq \max\Big\{\ |\alpha_1|,\ \ldots,\ |\alpha_N|\ \Big\} \\
&= \Big|\ \alpha_N\ \Big|
\end{aligned}$$

from which we have

$$\left|\ \sum_{i=1}^{N} \alpha_i\ \right| \ =\ \Big|\ \alpha_N\ \Big|. \tag{1.1.2}$$

We refer to equation (1.1.2) as *the case of equality in the strong triangle inequality.*

1.2 Completions

We say that $k, |\cdot|$ is *complete* if k is a complete metric space with respect to the metric topology induced by $|\cdot|$. A pair $(K, |\cdot|_K)$ consisting of a field K and an absolute value $|\cdot|_K$ is said to be a *completion* of the pair $(k, |\cdot|_k)$ if and only if

(i) K is complete with respect to $|\cdot|_K$,

(ii) there exists an isometric isomorphism of k onto a dense subfield of K.

The completions of a pair $(k, |\cdot|)$ are unique up to naturally defined isometric isomorphisms as described by Theorem M, Section 1.5 in [Rib99].

Theorem 1.2.1. (Uniqueness of Completions) *Let $(k, |\cdot|_k)$ be a pair consisting of a field k and an absolute value $|\cdot|_k$. Then there exists a pair $(K, |\cdot|_K)$ which is a completion of $(k, |\cdot|_k)$. Moreover, if $(K, |\cdot|_K)$ and $(L, |\cdot|_L)$ are both completions of $(k, |\cdot|_k)$, if $\sigma_K : k \to K$ and $\sigma_L : k \to L$ are the corresponding isometric isomorphisms, then there exists a unique isometric isomorphism $\tau : K \longrightarrow L$ such that $\tau \circ \sigma_K = \sigma_L$.*

Fields that are complete with respect to an archimedean absolute value satisfy the following characterization due to Ostrowski [Ost18].

Theorem 1.2.2. (Complete Archimedean Absolute Values) *Let K be a field which is complete with respect to an archimedean absolute value $|\cdot|_K$. Then there exists $\theta,\ 0 < \theta \leq 1$ such that $(K, |\cdot|_K)$ is isometrically isomorphic to $(\mathbb{R}, |\cdot|_\infty^\theta)$ or $(\mathbb{C}, |\cdot|_\infty^\theta)$.*

For the remainder of this section we assume that k is a field with nontrivial,

non-archimedean absolute value $|\cdot|$. We let K be a fixed completion of k and continue to use $|\cdot|$ for the extended absolute value on K and identify k with its image in K. We let v be the place of k containing $|\cdot|$ and V the place of K containing $|\cdot|$.

By Theorem 1.1.1 the following sets depend on v and V respectively and not on $|\cdot|$ alone. The notation $\mathcal{O}_v$, etc. is thus well defined.

$$\begin{aligned}
\mathcal{O}_v &= \Big\{\, \alpha \in k : |\alpha| \leq 1 \,\Big\}, \qquad \mathcal{O}_V = \Big\{\, \alpha \in K : \ |\alpha| \leq 1 \,\Big\} \\
\mathcal{U}_v &= \Big\{\, \alpha \in k : |\alpha| = 1 \,\Big\}, \qquad \mathcal{U}_V = \Big\{\, \alpha \in K : \ |\alpha| = 1 \,\Big\} \\
\mathcal{M}_v &= \Big\{\, \alpha \in k : |\alpha| < 1 \,\Big\}, \qquad \mathcal{M}_V = \Big\{\, \alpha \in K : \ |\alpha| < 1 \,\Big\}
\end{aligned}$$

Since $|\cdot|$ is non-archimedean, $\mathcal{O}_v$ is an integral domain, $\mathcal{U}_v$ is the multiplicative group of invertible elements in $\mathcal{O}_v$, and $\mathcal{M}_v$ is the unique maximal ideal of $\mathcal{O}_v$. The field $\mathbb{F}_v = \mathcal{O}_v \,/\, \mathcal{M}_v$ is called the *residue class field of* k. The residue class field of K, $\mathbb{F}_V$ is defined as $\mathbb{F}_V = \mathcal{O}_V \,/\, \mathcal{M}_V$.

An element $\alpha \in \mathcal{O}_v$ determines a coset $\alpha + \mathcal{M}_v$ in the residue class field $\mathbb{F}_v$. If $\alpha \in \mathcal{O}_v$ is viewed as an element of $\mathcal{O}_V$ it determines a coset $\alpha + \mathcal{M}_V$ in the residue class field $\mathbb{F}_V$. We can define the natural map

$$\psi : \mathbb{F}_v \longrightarrow \mathbb{F}_V \quad \text{given by} \quad \psi\{\, \alpha + \mathcal{M}_v \,\} = \alpha + \mathcal{M}_V$$

Let $\beta \in \mathcal{O}_V$. Since k is dense in K, there exists $\alpha \in k$ such that $|\alpha - \beta| < 1$. Then $|\alpha| \leq \max\{\, |\alpha - \beta|, \ |\beta| \,\} \leq 1$ so that $\alpha \in \mathcal{O}_v$ and $\alpha - \beta \in \mathcal{M}_V$. That is, $\psi(\alpha + \mathcal{M}_v) = \beta + \mathcal{M}_V$. This shows that ψ is surjective. ψ is an injective field homomorphism. Hence $\mathbb{F}_v \cong \mathbb{F}_V$.

Part of the research presented in this dissertation requires a careful understanding of the set

$$\left| \, k^{\times} \, \right| \; = \; \left\{ \; |\alpha| : \alpha \in k^{\times} \; \right\}$$

which is called the *multiplicative value group of* $(k, |\cdot|)$. Since $|\cdot|$ is a group homomorphism from the multiplicative group $k^{\times}$ to the multiplicative group of positive real numbers, $|k^{\times}|$ is a nontrivial subgroup of $(0, \infty)$. A nontrivial multiplicative subgroup $\mathrm{G} \leq (0, \infty)$ is either dense in $(0, \infty)$ or is discrete in which case it is an infinite cyclic group, $\mathrm{G} \; = \; \{ \; t^n : n \in \mathbb{Z} \; \}$ for some $t \; \in \; (0, 1)$. Since $\log : \; (\mathbb{R}^{+}, \times) \longrightarrow (\mathbb{R}, +)$ is a group isomorphism, this fact follows from Lemma 2.9.2 of [Koc00].

We say that $|\cdot|$ is *discrete* if its multiplicative value group is a discrete subgroup of $(0, \infty)$. It is clear that if $|\cdot|$ is discrete then all the absolute values in the place represented by $|\cdot|$ are also discrete. The extension of $|\cdot|$ to a completion K of k is also discrete and $|k^{\times}| = |K^{\times}|$. It will be useful to know, and it is easy to prove, that a nontrivial, non-archimedean absolute value on k is discrete if and only if $\mathcal{M}_v$ is a principal ideal of $\mathcal{O}_v$. Lemma 1.2.3 below follows from Lemma 3.3 in Chapter 1 of [Fes02] .

Lemma 1.2.3. (Uniformizing Parameters) *Let $|\cdot|$ be a discrete absolute value on k and let π be an element of the maximal ideal $\mathcal{M}_v$. Then the following are equivalent:*

(1) $\mathcal{M}_v \; = \; (\pi) \; = \; \{ \; \beta\pi \; : \; \beta \; \in \; \mathcal{O}_v \; \}$,

(2) $\sup \{ \; |\alpha| \; : \; \alpha \; \in \; \mathcal{M}_v \; \} \; = \; |\pi|$,

(3) the multiplicative value group of $(k, |\cdot|)$ is $\{ \; |\pi|^n \; : \; n \; \in \; \mathbb{Z} \; \}$.

An element π satifying the properties of the lemma is called a *prime* element or

a *uniformizing parameter*. Since $|k^\times| = |K^\times|$ and $k \subset K$, we have that a prime element for $(k, |\cdot|)$ is also a prime element for $(K, |\cdot|)$.

We require an understanding of how absolute values from a complete field $(\mathbb{K}, |\cdot|)$ are extended to a finite and seperable field extension $\mathbb{E}$ of $\mathbb{K}$. Let $[\mathbb{E} : \mathbb{K}] = n$. We recall the Norm map $N : \mathbb{E} \longrightarrow \mathbb{K}$. Let $\mathbb{V}$ be the Galois closure of $\mathbb{E}/\mathbb{K}$. That is $\mathbb{V}$ is the intersection of all Galois extensions of $\mathbb{K}$ that contain $\mathbb{E}$. Let $\mathrm{G} = \mathrm{Aut}(\ \mathbb{V}/\mathbb{K}\ )$, the *Galois group* of the extension $\mathbb{V}/\mathbb{K}$. Then $\mathbb{V}/\mathbb{E}$ is a Galois extension and $\mathrm{H} = \mathrm{Aut}(\ \mathbb{V}/\mathbb{E}\ ) \leq \mathrm{G}$. For $\beta \in \mathbb{E}$ we define

$$\mathrm{Norm}(\beta) \ = \ \mathrm{N}_{\mathbb{E}/\mathbb{K}}(\beta) \ = \ \prod_{\sigma} \sigma(\beta) \tag{1.2.1}$$

where the product is taken over a complete set of distinct coset representatives of H in G. Using $\mathrm{N}_{\mathbb{E}/\mathbb{K}} : \mathbb{E} \longrightarrow \mathbb{K}$ we can identify all extensions of $|\cdot|$ from $\mathbb{K}$ to $\mathbb{E}$ and as the following theorem shows there is actually one such extension. This theorem can be deduced from Section 4.5 of [Koc00].

Theorem 1.2.4. (Extensions of Absolute Values) *Let $\mathbb{K}$ be a field and $|\cdot|$ a nontrivial absolute value on $\mathbb{K}$. Suppose that $(\mathbb{K}, |\cdot|)$ is complete. Let $\mathbb{E}/\mathbb{K}$ be finite and seperable extension of fields of degree n. Then there exists a unique absolute value on $\mathbb{E}$, $||\cdot||$, that extends the absolute value $|\cdot|$ on $\mathbb{K}$. For all $\beta \in \mathbb{E}$ we have*

$$\Big|\Big| \ \beta \ \Big|\Big| \ = \ \Big| \ \mathrm{Norm}_{\mathbb{E}/\mathbb{K}}(\beta) \ \Big|^{1/n} \tag{1.2.2}$$

and $\mathbb{E}$ is complete in the metric topology induced by $||\cdot||$.

1.3 Absolute Values on the Rational Numbers

We describe all the absolute values on the field $\mathbb{Q}$ of rational numbers. Let $\mathcal{A}_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$. Let $|\cdot|_\infty$ be the usual archimedean absolute value on $\mathbb{Q}$. For each prime number p there exist the usual p-adic absolute value defined in the following way. By The Fundamental Theorem of Arithmetic, a nonzero rational number β can be written as

$$\beta = \pm 2^{\tau_2(\beta)} 3^{\tau_3(\beta)} 5^{\tau_5(\beta)} 7^{\tau_7(\beta)} \cdots , \tag{1.3.1}$$

where $\{\tau_q(\beta)\}$ is a sequence of integers indexed by the set of prime numbers q and where $\tau_q(\beta) = 0$ for all but finitely many primes. The usual p-adic absolute value on $\mathbb{Q}^\times$ is defined by

$$\Big| \beta \Big|_p = \begin{cases} p^{-\tau_p(\beta)} & \text{if } \beta \neq 0 \\ 0 & \text{if } \beta = 0 \end{cases}$$

Since

$$\Big| \mathbb{Q}^\times \Big|_p = \Big\{ p^n \ : \ n \in \mathbb{Z} \Big\} \tag{1.3.2}$$

it follows that $|\cdot|_p$ are discrete absolute values with uniformizing parameters p. We have

$$\begin{aligned} \mathcal{O}_p &= \Big\{ \beta \in \mathbb{Q} \ : \ |\beta|_p \leq 1 \Big\} = \Big\{ a/b \in \mathbb{Q} \ : \ p \nmid b \Big\} \\ \mathcal{M}_p &= \Big\{ \beta \in \mathbb{Q} \ : \ |\beta|_p < 1 \Big\} = \Big\{ a/b \in \mathbb{Q} \ : \ p \nmid b \text{ and } p \mid a \Big\} \end{aligned}$$

and it is easy to show that the residue class field $\mathcal{O}_p \ / \ \mathcal{M}_p$ is isomorphic to the field $\mathbb{F}_p \equiv \mathbb{Z}/p\mathbb{Z}$. In this dissertation, for a rational prime q, $\mathbb{F}_q$ will denote the finite field

$\mathbb{Z}/q\mathbb{Z}$.

It follows from Theorem 1.1.1 that the absolute values $|\cdot|_\infty,\ |\cdot|_2,\ |\cdot|_3,\ \ldots .$ are pairwise inequivalent and thus represent distinct places of $\mathcal{A}_\mathbb{Q}$. It is a theorem of Ostrowski [Ost18] that these absolute values form a complete set of equivalence class representatives for $\mathcal{A}_\mathbb{Q}$.

Theorem 1.3.1. (The Places of $\mathbb{Q}$) Let $\mathcal{A}_\mathbb{Q}$ be the set of places of $\mathbb{Q}$. For $p \in \{\ \infty,\ 2,\ 3,\ \ldots\ \}$ the absolute values $|\cdot|_p$ form a complete set of (pairwise inequivalent) representatives of $\mathcal{A}_\mathbb{Q}$.

We can easily see that for any $\alpha\ \in\ \mathbb{Q}^\times$

$$\prod_{\mathcal{A}_\mathbb{Q}} |\ \alpha\ |_u\ =\ 1 \tag{1.3.3}$$

This fact is called the *Product Formula* for $\mathbb{Q}$.

1.4 Valuations

Let k be a field. A *valuation* on k is a map $\nu : k \longrightarrow \mathbb{R} \bigcup \{\ \infty\ \}$ that satisfies each of the following properties

(i) $\nu(\ x\ )\ =\ \infty$ if and only if $x = 0$,

(ii) $\nu(\ x \cdot y\ )\ =\ \nu(x) + \nu(y)$ for all $x,\ y\ \in\ k$,

(iii) $\nu(\ x + y\ )\ \geq\ \min\Big\{\ \nu(x),\ \nu(y)\ \Big\}$ for all $x,\ y\ \in\ k$.

If ν is a valuation on k then the set $\{ \alpha \in k : \nu(\alpha) \geq 0 \} \bigcup \{ 0 \}$ is called the *valuation ring of* ν. There exists a one-to-one correspondence between the non-archimedean absolute values on k and the valuations on k. Let ν be a valuation on k and θ a positive real number. Then $|\cdot| : k \longrightarrow [0, \infty)$ defined by $|x| = e^{-\theta \cdot \nu(x)}$ defines a non-archimedean absolute value on k. If $|\cdot|$ is a non-archimedean absolute value on k, then $\nu : k \longrightarrow \mathbb{R} \bigcup \{ \infty \}$ defined by

$$\nu(x) = \begin{cases} -\theta \cdot \log |x| & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}$$

is a valuation on k. We note that there exists no correspondence of this kind between archimedean absolute values on k and valuations on k.

From these remarks, we see that all the ideas developed for non-archimedean absolute values on k also apply to valuations on k. In particular, if ν is a valuation on k and θ a positive real number then the map $(x, y) : k \times k \longrightarrow [0, \infty)$ defined by

$$(x, y) = \begin{cases} e^{-\theta \cdot \nu(x-y)} & \text{if } x \neq y \\ 0 & \text{if } x = y \end{cases}$$

is a metric and induces a metric topology on k. We say that two valuations ν_1 and ν_2 are equivalent if they induce the same metric topology on k. By Theorem 1.1.1, we have that ν_1 and ν_2 are equivalent if and only if

$$\left\{ x \in k : \nu_1(x) > 0 \right\} = \left\{ x \in k : \nu_2(x) > 0 \right\}$$

If ν is a nontrivial valuation on k then $\nu : k^\times \longrightarrow \mathbb{R}$ is a group homomorphism from the multiplicative group $k^\times$ to the additive group of real numbers. The image

$$\nu\Big(\ k^\times \ \Big) \ = \ \Big\{ \ \nu(\alpha) \ : \ \alpha \ \in \ k^\times \ \Big\}$$

is a nontrivial subgroup and is called the *additive value group* of (k, ν). A valuation ν is said to be a *discrete valuation* if its additive value group is a discrete subgroup. A valuation ν is discrete if and only if there exists a positive number θ such that the equivalent valuation $x \longrightarrow \theta \cdot \nu(x)$ has additive value group equal to $\mathbb{Z}$.

As an example, suppose that β is a nonzero rational number,

$$\beta \ = \ \pm 2^{\tau_2(\beta)} 3^{\tau_3(\beta)} 5^{\tau_5(\beta)} 7^{\tau_7(\beta)} \cdots ,$$

Then the usual p-adic absolute value of β is

$$\Big| \ \beta \ \Big|_p \ = \ p^{-\tau_p(\beta)}$$

If we extend the map $\tau_p : \mathbb{Q}^\times \longrightarrow \mathbb{Z}$ by setting $\tau_p(0) = \infty$, then $\tau_p : \mathbb{Q} \longrightarrow \mathbb{R} \bigcup \{\infty\}$ is a valuation on $\mathbb{Q}$.

1.5 The Places of an Algebraic Number Field

Let $\mathbb{K}$ be an algebraic number field of degree d over $\mathbb{Q}$. Let v be a place of $\mathbb{K}$ and let u be the place of $\mathbb{Q}$ to which v restricts. We define the *local degree of* v as

$$d_v \ \equiv \ [\ \mathbb{K}_v \ : \ \mathbb{Q}_u \ ]$$

We choose to identify two absolute values within v that will be useful. First assume that v is an archimedean place. There exists a unique absolute value, $||\cdot||_v \in v$ that restricts to the absolute value $|\cdot|_\infty$ on $\mathbb{Q}$. If v is a non-archimedean place then there exists a rational prime p such that v restricts to the p-adic place of $\mathbb{Q}$. We let $||\cdot||_v$ be the unique absolute value in v that restricts to the absolute value $|\cdot|_p$ on $\mathbb{Q}$. For each place v of $\mathbb{K}$, archimedean or non-archimedean, we then define

$$\left|\cdot\right|_v = \left|\left|\cdot\right|\right|_v^{d_v/d} \tag{1.5.0}$$

Let $\mathbb{K} \subseteq \mathbb{E}$ be an extension of algebraic number fields. Let u be a non-archimedean place of $\mathbb{K}$ and v a non-archimedean place of $\mathbb{E}$ restricting to u on $\mathbb{K}$. We require the following explicit characterization of $||\cdot||_v$ in terms of $||\cdot||_u$. The following theorem is a specialization of that found as Theorem 2.6 of [Fes02].

Theorem 1.5.1. (The Non-Archimedean Places) *Let $\mathbb{K} \subseteq \mathbb{E}$ be algebraic number fields. Let $\alpha \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{K}(\alpha)$. Let u be a non-archimedean place of $\mathbb{K}$ and let v be a non-archimedean place of $\mathbb{E}$ such that v restricts to u on $\mathbb{K}$. Let $\mathbb{K}_u$ be the completion of $\mathbb{K}$ with respect to u and let $\widehat{||\cdot||}_u$ be the extension of $||\cdot||_u$ on $\mathbb{K}$ to $\mathbb{K}_u$. Let $m_{\alpha,\mathbb{K}}(x) = \prod_{i=1}^{t} s_i(x)$ be the unique factorization of the minimal polynomial of α over $\mathbb{K}[x]$ into monic irreducibles over $\mathbb{K}_u[x]$. For α_i $(\alpha = \alpha_1)$ a root of $s_i(x)$ let $\mathbb{E}_i = \mathbb{K}_u(\alpha_i)$. Let $\widehat{||\cdot||}_{v_i}$ be the unique extension* (defined by Theorem 1.2.4) *of $\widehat{||\cdot||}_u$ to $\mathbb{E}_i$.*

Then $\mathbb{E}$ is embedded as a dense subfield of the complete field $\mathbb{E}_i$ by $\mathbb{K} \hookrightarrow \mathbb{K}_u$ and $\alpha \longrightarrow \alpha_i$ and the restriction $||\cdot||_{v_i}$ of $\widehat{||\cdot||}_{v_i}$ to $\mathbb{E}$ is a non-archimedean absolute value restricting to $||\cdot||_u$ on $\mathbb{K}$. The absolute values $||\cdot||_{v_i}$ are distinct and every absolute value on $\mathbb{E}$ restricting to $||\cdot||_u$ on $\mathbb{K}$ corresponds to one of these.

The archimedean places on $\mathbb{K}$ are described by the following theorem (Theorem 4.8.3 of [Koc00]). In the following $||\cdot||_\infty$ will denote the usual archimedean absolute value on $\mathbb{C}$.

Theorem 1.5.2. (The Archimedean Places) *Let $|\cdot|_\infty$ be the usual archimedean absolute value on $\mathbb{Q}$. Let $\mathbb{K}$ be an algebraic number field of degree d over $\mathbb{Q}$ and let $g_1, \ldots g_{r_1}$ be the real isomorphisms and $(g_{r_1+1}, g_{r_1+r_2+1}), \ldots, (g_{r_1+r_2}, g_d)$ the pairs of complex conjugate isomorphisms of $\mathbb{K}$ into $\mathbb{C}$ we then obtain all the extensions $||\cdot||_v$ of $|\cdot|_\infty$ to $\mathbb{K}$ by*

$$\left|\left|\ \alpha\ \right|\right|_v\ =\ \left|\left|\ g_i\alpha\ \right|\right|_\infty \text{ for } \alpha\ \in\ \mathbb{K},\ i\ =\ 1,\ \ldots,\ r_1+r_2 \tag{1.5.1}$$

We now allow for $p\ \in\ \{\ \infty,\ 2,\ 3,\ 5,\ \ldots\ \}$. Let $\mathcal{A}_p\ =\ \{\ v_1,\ \ldots,\ v_k\ \}$ denote the set of places of $\mathbb{K}$ restricting to the p-adic place on $\mathbb{Q}$. From Theorems 1.5.1 and 1.5.2 we have the following identity

$$\sum_{\mathcal{A}_p} d_v\ =\ d \tag{1.5.2}$$

From Theorems 1.5.1 and 1.5.2 for $\alpha\ \in\ \mathbb{K}$ we have

$$\text{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha)\ =\ \prod_{\mathcal{A}_p} \text{Norm}_{\mathbb{K}_v/\mathbb{Q}_p}(\alpha) \tag{1.5.3}$$

and by using Theorem 1.2.4 we have for $v\ \in\ \mathcal{A}_p$,

$$\left|\left|\ \alpha\ \right|\right|_v\ =\ \left|\ \text{Norm}_{\mathbb{K}_v/\mathbb{Q}_p}(\alpha)\ \right|_p^{1/d_v} \tag{1.5.4}$$

and since $\left|\ \alpha\ \right|_v\ =\ \left|\left|\alpha\right|\right|_v^{d_v/d}$ we have

$$\left|\ \alpha\ \right|_v\ =\ \left|\ \mathrm{Norm}_{\mathbb{K}_v/\mathbb{Q}_p}(\alpha)\ \right|_p^{1/d} \tag{1.5.5}$$

from which we obtain the identity

$$\prod_{\mathcal{A}_p} |\alpha|_v\ =\ \left|\ \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha)\ \right|_p^{1/d} \tag{1.5.6}$$

Let $\alpha \in \overline{\mathbb{Q}}^{\times}$, let $\mathbb{K}$ be an algebraic number field containing α, let $\mathcal{A}_{\mathbb{K}}$ be the set of places of $\mathbb{K}$, let $\mathcal{A}_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$ and for $p \in \mathcal{A}_{\mathbb{Q}}$ let $\mathcal{A}_p$ be the set of places of $\mathbb{K}$ that restrict to p on $\mathbb{Q}$. Then

$$\begin{aligned}
\prod_{\mathcal{A}_{\mathbb{K}}} |\alpha|_v\ &=\ \prod_{\mathcal{A}_{\mathbb{Q}}} \Big\{\ \prod_{\mathcal{A}_p} |\alpha|_v\ \Big\} \\
&=\ \Big\{\ \prod_{\mathcal{A}_{\mathbb{Q}}} \Big|\ \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha)\ \Big|_p\ \Big\}^{1/d} \\
&=\ 1
\end{aligned}$$

We record this result as a theorem and refer to it as the *Product Formula*.

Theorem 1.5.3. (Product Formula) *Let $\mathbb{K}$ be an algebraic number field, $\alpha\ \in\ \mathbb{K}^{\times}$ and let $\mathcal{A}_{\mathbb{K}}$ be the set of places of $\mathbb{K}$. Then*

$$\prod_{\mathcal{A}_{\mathbb{K}}} \left|\ \alpha\ \right|_v\ =\ 1 \tag{1.5.7}$$

1.6 The Galois Action on Places

Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension and let $\mathrm{G} = \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $\mathcal{A}_{\mathbb{K}}$ be the set of places of $\mathbb{K}$, $\mathcal{A}_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$ and for $p \in \mathcal{A}_{\mathbb{Q}}$ let $\mathcal{A}_p$ be the set of places of $\mathbb{K}$ that restrict to p on $\mathbb{Q}$. Let $v \in \mathcal{A}_{\mathbb{K}}$ and let $\sigma \in \mathrm{G}$. The map $|\cdot|_{\sigma v} : \mathbb{K} \longrightarrow [0, \infty)$ defined by

$$\left| \ \alpha \ \right|_{\sigma v} = \left| \ \sigma^{-1}(\alpha) \ \right|_v \tag{1.6.1}$$

is an absolute value on $\mathbb{K}$. Since σ fixes $\mathbb{Q}$, $|\cdot|_v$ and $|\cdot|_{\sigma v}$ restrict to the same absolute value on $\mathbb{Q}$. If $\tau \in \mathrm{G}$ then

$$\begin{aligned} \left| \ \alpha \ \right|_{(\sigma\tau)v} &= \left| \ (\sigma\tau)^{-1}\alpha \ \right|_v \\ &= \left| \ \tau^{-1}\sigma^{-1}(\alpha) \ \right|_v \\ &= \left| \ \sigma^{-1}(\alpha) \right|_{\tau v} \\ &= \left| \ \alpha \ \right|_{\sigma(\tau v)} \end{aligned}$$

which shows that equation (1.6.1) defines a group action of G on $\mathcal{A}_p$ for $p \in \mathcal{A}_{\mathbb{Q}}$. From Theorems 1.5.1 and 1.5.2 we can deduce the following.

Theorem 1.6.1. (Galois Action on Places) *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension. Let $\mathcal{A}_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$. For $p \in \mathcal{A}_{\mathbb{Q}}$ let $\mathcal{A}_p$ be the set of places of $\mathbb{K}$ that restrict to p on $\mathbb{Q}$. Then* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$ *acts transitively on $\mathcal{A}_p$.*

1.7 Ideals and Valuations of Algebraic Number Fields

First we recall the meaning of a *localization*. Let R be an integral domain and P a nonzero prime ideal of R. The localization of R at P is denoted R_P and is equal to the ring

$$R_P \;=\; \left\{ \frac{a}{b} \;: a \in R \text{ and } b \;\in\; R - P \right\} \tag{1.7.1}$$

Let $\mathbb{K}$ be an algebraic number field. An element $\alpha \;\in\; \mathbb{K}$ is said to be an *algebraic integer* if α is the root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers in $\mathbb{K}$ forms a ring and is denoted $\mathcal{O}_{\mathbb{K}}$.

Lemma 1.7.0. **($\mathcal{O}_{\mathbb{K}} = \bigcap_{v \nmid \infty} \mathcal{O}_v$)** *Let $\mathbb{K}$ be an algebraic number field. Then*

$$\mathcal{O}_{\mathbb{K}} = \bigcap_{v \nmid \infty} \mathcal{O}_v \tag{1.7.2}$$

Proof. Lemma 1.7.0 is a consequence of equations (3.1.6), (3.1.7) and (3.1.17) □

$\mathcal{O}_{\mathbb{K}}$ is a Dedekind Domian (Proposition 14, Section 15.3 of [Dum99]). We list several implications of this fact which are described in Sections 15.3, 15.4, 16.2, and 16.3 of [Dum99].

Theorem 1.7.1. **(Properties of $\mathcal{O}_{\mathbb{K}}$)** *Let $n \in \mathbb{N}$ and let $\mathbb{K}$ be an algebraic number field of degree n over $\mathbb{Q}$ and let $\mathcal{O}_{\mathbb{K}}$ be the ring of integers of $\mathbb{K}$. Then*

(i) Every nonzero prime ideal of $\mathcal{O}_{\mathbb{K}}$ is maximal.

(ii) $\mathbb{K}$ is the field of fractions of $\mathcal{O}_{\mathbb{K}}$.

(iii) *Every nonzero proper ideal I of $\mathcal{O}_{\mathbb{K}}$ can be written as a finite product of prime ideals:*

$$I = \mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_t \quad \textit{(not necessarily distinct)}$$

where the set of primes is uniquely determined and so every nonzero proper ideal I of $\mathcal{O}_{\mathbb{K}}$ can be written uniquely (up to order) as a product of powers of prime ideals.

(iv) *Given $\alpha \in \mathbb{K}$ there exists $d \in \mathbb{N}$ such that $d \cdot \alpha \in \mathcal{O}_{\mathbb{K}}$.*

(v) *The localization of $\mathcal{O}_{\mathbb{K}}$ at a prime ideal is a discrete valuation ring for some discrete valuation ν on $\mathbb{K}$*

(vi) *If ν is a discrete valuation on $\mathbb{K}$ then $\mathcal{P} = \{\ \alpha \in \mathcal{O}_{\mathbb{K}} : \nu(\alpha) > 0\ \}$ is a prime ideal of $\mathcal{O}_{\mathbb{K}}$ and the localization of $\mathcal{O}_{\mathbb{K}}$ at the prime ideal $\mathcal{P}$ corresponds to the discrete valuation ring of ν.*

(vii) *$\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$ module of degree $[\mathbb{K} : \mathbb{Q}]$.*

For each non-archimedean place v of $\mathbb{K}$ we wish to explicitly characterize the absolute value $|\cdot|_v$ in terms of its naturally associated discrete valuation ring . We first note the following lemma whose proof is a simple exercise. (Lemma 1.7.2 was contained in [Val07].)

Lemma 1.7.2. (Absolute Values on Integral Domains) *Let R be an integral domain and let K be its field of fractions. Assume that the map $||\cdot|| : R \longrightarrow [0,\infty)$ satisfies the following three conditions*

(1) $||x|| = 0$ if and only if $x = 0$,

(2) $||x \cdot y|| = ||x|| \cdot ||y||$ for all x and $y \in R$

(3) $\big|\big|\ x+y\ \big|\big| \ \leq\ ||x||+||y||$ for all x and $y\ \in\ R$

Then there exists a unique absolute value $|\cdot|\ :\ K\longrightarrow[0,\infty)$ *such that* $|x|=||x||$ *for all* $x\ \in\ R$. *If* $||\cdot||$ *satisfies the strong triangle inequality*

(4) $\big|\big|\ x+y\ \big|\big| \leq \max\Big\{\ ||x||,\ ||y||\ \Big\}$ *for all* x *and* $y\ \in\ R$,

then $|\cdot|$ *on* K *is a non-archimedean absolute value. If* a *and* $b\neq 0$ *are in* R *and* $a/b\ \in\ K$ *then*

$$\left|\ \frac{a}{b}\ \right|\ =\ \frac{||a||}{||b||} \tag{1.7.3}$$

It is clear that an absolute value on $\mathbb{K}$ induces a map on $\mathcal{O}_{\mathbb{K}}$ satisfying the properties listed in Lemma 1.7.2. Consequently, since $\mathbb{K}$ is the field of fractions of $\mathcal{O}_{\mathbb{K}}$ we need only find all maps $||\cdot||\ :\ \mathcal{O}_{\mathbb{K}}\longrightarrow[0,\infty)$ that satisfy the properties listed in Lemma 1.7.2. To this end suppose that $||\cdot||$ is such a map and by Lemma 1.7.2. is associated to a place v of $\mathbb{K}$. Then the set $\mathfrak{B}_1\ =\ \{\ \alpha\ \in\ \mathcal{O}_{\mathbb{K}}\ :\ ||\alpha||<1\ \}$ is seen to be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ that depends on the place v containing $|\cdot|$ and not on $||\cdot||$ itself. Let $p\ \in\ \mathbb{N}$ be the unique rational prime such that $\mathfrak{B}_1\ \bigcap\ \mathbb{Z}\ =\ p\mathbb{Z}$. Let $\mathcal{A}_p$ be the set of places of $\mathbb{K}$ that restrict to the $p-$adic place of $\mathbb{Q}$. We see that $p\mathcal{O}_{\mathbb{K}}\ \subseteq\ \mathfrak{B}_1\mathcal{O}_{\mathbb{K}}$. Let $\mathfrak{I}_p\ =\ \{\ \mathfrak{B}_1,\ \ldots\ ,\ \mathfrak{B}_t\ \}$ be the set of prime ideals of $\mathcal{O}_{\mathbb{K}}$ such that $\mathfrak{B}_i\ \bigcap\ \mathbb{Z}\ =\ p\mathbb{Z}$ and let $\{\ e_1,\ \ldots\ ,\ e_t\ \}\ \subset\ \mathbb{N}\ \bigcup\ \{0\}$. Suppose that $p\mathcal{O}_{\mathbb{K}}\ =\ \mathfrak{B}_1^{e_1}\cdots\mathfrak{B}_t^{e_t}$. Define $\nu_{\mathfrak{B}_1}\ :\ \mathcal{O}_{\mathbb{K}}^{\times}\longrightarrow\mathbb{N}$ as follows. For $\alpha\ \in\ \mathcal{O}_{\mathbb{K}}^{\times}$ and $n_1\ \in\mathbb{N}\ \bigcup\ \{\ 0\ \}$ the maximal power of $\mathfrak{B}_1$ in the unique factorization of the ideal $\alpha\mathcal{O}_{\mathbb{K}}$ into a product of powers of prime ideals as in (iii) of Theorem 1.8.1, let

$$\nu_{\mathfrak{B}_1}(\alpha)=n_1 \tag{1.7.4}$$

Then $||\alpha||_{\mathfrak{B}_1}=p^{-\nu_{\mathfrak{B}_1}(\alpha)}$ defines a map of from $\mathcal{O}_{\mathbb{K}}$ to $[0,\infty)$ satisfying the properties

listed in Lemma 1.7.2. We see that the induced absolute value on $\mathbb{K}$ is in the same place as the absolute value induced by the map $||\cdot||$. Since $\nu_{\mathfrak{B}_1}(p) = e_1$ it follows that $||\beta||_v = p^{-\frac{1}{e_1}\nu_{\mathfrak{B}_1}(\beta)}$ for all $\beta \in \mathcal{O}_{\mathbb{K}}^{\times}$. We thus have a simple characterization of the absolute values $||\cdot||_v$ for non-archimedean places v in terms of the unique prime ideal factorization of $p\mathcal{O}_{\mathbb{K}}$ where $v \in \mathcal{A}_p$.

1.8 Decomposition Groups of Prime Ideals in $\mathcal{O}_{\mathbb{K}}$

Let $p \in \mathbb{N}$ be a rational prime. Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension and set $\mathrm{G} = \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $\mathcal{A}_p = \{\ v_1,\ \ldots,\ v_t\ \}$ (where $t \in \mathbb{N}$) be the finite set of places of $\mathbb{K}$ restricting to the unique place of $\mathbb{Q}$ containing $|\cdot|_p$. For $v_i \in \mathcal{A}_p$ let $\mathfrak{B}_i = \{\ \alpha \in \mathcal{O}_{\mathbb{K}} : |\alpha|_{v_i} < 1\ \}$. Then $\mathfrak{I}_p = \{\ \mathfrak{B}_1,\ \ldots,\ \mathfrak{B}_t\ \}$ is the complete set of prime ideals of $\mathcal{O}_{\mathbb{K}}$ such that $\mathfrak{B}_i \bigcap \mathbb{Z} = p\mathbb{Z}$. As $\mathfrak{B}_i \in \mathfrak{I}_p$ is a prime and thus maximal ideal of $\mathcal{O}_{\mathbb{K}}$ and $p \in \mathfrak{B}_i$, the field $\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i$ is clearly of characteristic p and by property (vii) of Theorem 1.7.1 we can see that $[\ (\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i) : \mathbb{F}_p\ ]$ is finite. From basic Algebra we know that $[\ (\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i) : \mathbb{F}_p\ ]$ is a cyclic Galois extension. We will denote $\mathrm{G}_{\mathfrak{B}_i} = \mathrm{Aut}\Big(\ (\ \mathcal{O}_{\mathbb{K}}\ /\ \mathfrak{B}_i\ )/\ \mathbb{F}_p\ \Big)$. We set $f = [(\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i) : \mathbb{F}_p]$ and refer to f as the *residue class degree* of $\mathfrak{B}_i$. It is a fact (Theorem 6.1.1 of [Koc00]) that there exists $e \in \mathbb{N}$ such that

$$p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{t} \mathfrak{B}_i^e \tag{1.8.1}$$

We call e the *ramification index* of p in $\mathbb{K}$. It also follows from Theorem 6.1.1 of [Koc00] that for all $\mathfrak{B}_i$ and $\mathfrak{B}_j \in \mathfrak{I}_p$, $[\ (\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i) : \mathbb{F}_p\ ] = [\ (\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_j) : \mathbb{F}_p\ ]$. We thus refer to this quantity as the residue class degree of p in $\mathbb{K}$.

Given $g \in \mathrm{G}$ and $\mathfrak{B}_i \in \mathfrak{I}_p$ we define

$$g(\mathfrak{B}_i) = \Big\{\ g(\alpha) : \alpha \in \mathfrak{B}_i\ \Big\} \tag{1.8.2}$$

and we note that $g(\mathfrak{B}_i) \in \mathfrak{I}_p$. We define the *decomposition group of* $\mathfrak{B}_i$ as

$$\mathrm{Z}_{\mathfrak{B}_i} = \left\{ g \in \mathrm{G} : g(\mathfrak{B}_i) = \mathfrak{B}_i \right\} \tag{1.8.3}$$

and note that $\mathrm{Z}_{\mathfrak{B}_i} \leq \mathrm{G}$.

We define the *inertia group of* $\mathfrak{B}_i$ as

$$\mathrm{G}_{\mathfrak{B}_i,0} = \left\{ g \in \mathrm{G} : \alpha - g(\alpha) \in \mathfrak{B}_i \text{ for all } \alpha \in \mathcal{O}_{\mathbb{K}} \right\} \tag{1.8.4}$$

and note that $\mathrm{G}_{\mathfrak{B}_i,0} \trianglelefteq \mathrm{Z}_{\mathfrak{B}_i}$.

For $n \in \mathbb{N}$ we define the *n-th ramification group of* $\mathfrak{B}_i$ as

$$\mathrm{G}_{\mathfrak{B}_i,n} = \left\{ g \in \mathrm{G} : \alpha - g(\alpha) \in \mathfrak{B}_i^{n+1} \text{ for all } \alpha \in \mathcal{O}_{\mathbb{K}} \right\} \tag{1.8.5}$$

and we note that for all $n \in \mathbb{N}$ we have $\mathrm{G}_{\mathfrak{B}_i,n} \trianglelefteq \mathrm{G}_{\mathfrak{B}_i,n-1}$. We now state as a theorem many properties of decompostion groups that we will use later and whose proof can be found in Section 6.1 of [Koc00].

Theorem 1.8.1. (Properties of Decomposition Groups) *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension,* $\mathrm{G} = \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ and $p \in \mathbb{N}$ *a rational prime with ramification index* e *and residue class degree* f *in* $\mathbb{K}$. *Let* $\mathfrak{I}_p = \{ \mathfrak{B}_1, \ldots, \mathfrak{B}_t \}$ *(where* $t \in \mathbb{N}$ *) be the finite set of prime ideals of* $\mathcal{O}_{\mathbb{K}}$ *such that* $\mathfrak{B}_i \bigcap \mathbb{Z} = p\mathbb{Z}$. *Then*

(i) G *acts transitively on* $\mathfrak{I}_p$ *and for* $\mathfrak{B}_i$ *and* $\mathfrak{B}_j \in \mathfrak{I}_p$ *and* $g \in \mathrm{G}$ *such that* $g(\mathfrak{B}_i) = \mathfrak{B}_j$ *we have* $g\mathrm{Z}_{\mathfrak{B}_i} g^{-1} = \mathrm{Z}_{\mathfrak{B}_j}$,

(ii) *For all* $\mathfrak{B}_i \in \mathfrak{I}_p$ *we have* $\left| \mathrm{G}_{\mathfrak{B}_i,0} \right| = e$, $\mathrm{Z}_{\mathfrak{B}_i} / \mathrm{G}_{\mathfrak{B}_i,0}$ *is cyclic of degree* f *and* $\mathrm{G}_{\mathfrak{B}_i} = \mathrm{Z}_{\mathfrak{B}_i} / \mathrm{G}_{\mathfrak{B}_i,0}$

(iii) $G_{\mathfrak{B}_i,n} = \{ 1 \}$ *for sufficiently large* $n \in \mathbb{N}$,

(iv) *There exists an injective homomorphism*

$$\phi : G_{\mathfrak{B}_i,0} / G_{\mathfrak{B}_i,1} \longrightarrow \Big(\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i \Big)^{\times}$$

(v) *For all* $n \in \mathbb{N}$, *there exists an injective homomorphism*

$$\psi : G_{\mathfrak{B}_i,n} / G_{\mathfrak{B}_i,n+1} \longrightarrow \Big(\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i \Big)^{+}$$

From property (iv) we see that $G_{\mathfrak{B}_i,0} / G_{\mathfrak{B}_i,1}$ is a cyclic group whose order is a divisor of $p^f - 1$ and that $G_{\mathfrak{B}_i,1}$ is the unique Sylow-p subgroup of $G_{\mathfrak{B}_i,0}$. From property (v) we see that $G_{\mathfrak{B}_i,n} / G_{\mathfrak{B}_i,n+1}$ is a finite abelian group of exponent p. From property (ii) and by considering the sequence

$$Z_{\mathfrak{B}_i} \supseteq G_{\mathfrak{B}_i,0} \supseteq G_{\mathfrak{B}_i,1} \supseteq \cdots \supseteq G_{\mathfrak{B}_i,m} = \{ 1 \} \tag{1.8.6}$$

we can see that the decomposition group $Z_{\mathfrak{B}_i}$ is solvable.

Let $\phi : Z_{\mathfrak{B}_i} \longrightarrow Z_{\mathfrak{B}_i} / G_{\mathfrak{B}_i,0}$ be the natural projection homomorphism. If $g \in G$ such that $\langle \phi(g) \rangle = Z_{\mathfrak{B}_i}$ then will will say that g *acts as the Frobenius automorphism on* $\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i$. If $\alpha \in \mathcal{O}_{\mathbb{K}}$ and $\langle \phi(g) \rangle = Z_{\mathfrak{B}_i}$ then from elementary Algebra $g(\alpha) - \alpha^p \in \mathfrak{B}_i$. In coset notation, $\phi(g)(\overline{\alpha}) = \overline{\alpha}^p$ and if $[(\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i) : \mathbb{F}_p] = m$ then $\alpha^{p^m} - \alpha \in \mathfrak{B}_i$.

1.9 The Stabilizer of a non-Archimedean Place of $\mathbb{K}$

Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension and let $G \equiv \text{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $p \in \mathbb{N}$ be a rational prime and let $\mathcal{A}_p = \{\ v_1,\ \ldots\ ,\ v_t\ \}$ (where $t \in \mathbb{N}$) be the finite set of places of $\mathbb{K}$ extending the place of $\mathbb{Q}$ represented by $|\cdot|_p$. For each $v_i \in \mathcal{A}_p$ let $\mathfrak{B}_i = \{\ \alpha \in \mathcal{O}_{\mathbb{K}} : |\alpha|_p < 1\ \}$. Then $\mathfrak{I}_p = \{\ \mathfrak{B}_1,\ \ldots\ ,\ \mathfrak{B}_t\ \}$ is the complete set of prime ideals of $\mathcal{O}_{\mathbb{K}}$ such that $\mathfrak{B}_i \bigcap \mathbb{Z} = p\mathbb{Z}$.

Consider the injection

$$\psi : \mathcal{O}_{\mathbb{K}} / \mathfrak{B}_i \longrightarrow \mathbb{F}_{v_i} \tag{1.9.1}$$

defined by

$$\psi(\alpha + \mathfrak{B}_i) = \alpha + \mathcal{M}_{v_i}$$

we see that

$$[(\ \mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i\ ) : \mathbb{F}_p] \leq [\ \mathbb{F}_{v_i} : \mathbb{F}_p]$$

Now let $\beta \in \mathcal{O}_{v_i}$. By (v) and (vi) of Theorem 1.7.1 there exist $a,\ b \in \mathcal{O}_{\mathbb{K}}$ such that $\beta = a/b$ and $|b|_{v_i} = 1$. Let $m = [(\ \mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i\ ) : \mathbb{F}_p]$. and consider the equation

$$\begin{aligned}(a/b)^{p^m} - (a/b) &= (b \cdot a^{p^m} - a \cdot b^{p^m})/(b^m \cdot b) \\ &= \left((a^{p^m} - a)(b + b^{p^m}) - (ab)^{p^m} + ab\right)/(b^{p^m} \cdot b)\end{aligned}$$

Since $(ab)^{p^m} - ab \in \mathcal{M}_{v_i}$, $a^{p^m} - a \in \mathcal{M}_{v_i}$, $b^{p^m+1} \in \mathcal{U}_{v_i}$, and $b^{p^m} + b \in \mathcal{O}_{v_i}$ we see that $\beta^{p^m} - \beta \in \mathcal{M}_{v_i}$.

As a result

$$[(\ \mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i\ ) : \mathbb{F}_p\ ] \geq [\ \mathbb{F}_{v_i} : \mathbb{F}_p\ ]$$

and so

$$[(\ \mathcal{O}_{\mathbb{K}}/\mathfrak{B}_i\ )\ :\ \mathbb{F}_p] \ =\ [\ \mathbb{F}_{v_i}\ :\ \mathbb{F}_p\ ] \tag{1.9.2}$$

Thus the injection in equation (1.9.1) is a surjection and consequently a field isomorphism. We can thus set

$$\mathrm{G}_{v_i} = \mathrm{G}_{\mathfrak{B}_i} = \mathrm{Aut}(\ \mathbb{F}_{v_i}\ /\ \mathbb{F}_p\ ) \tag{1.9.3}$$

We define the *stabilizer* of the place $v_i\ \in\ \mathcal{A}_p$ as

$$\mathrm{Z}_{v_i}\ =\ \left\{\ \sigma\ \in\ \mathrm{G}\ :\ |\cdot|_{\sigma v_i}\ =\ |\cdot|_{v_i}\ \right\} \tag{1.9.4}$$

and we can easily show that $\mathrm{Z}_{v_i}\ =\ \mathrm{Z}_{\mathfrak{B}_i}$.

We define the *inertia group* of v_i as

$$\mathrm{G}_{v_i,0}\ =\ \left\{\ \sigma\ \in\ \mathrm{G}\ :\ \sigma(\alpha)-\alpha\ \in\ \mathcal{M}_{v_i}\ \text{for all}\ \alpha\ \in\ \mathcal{O}_{v_i}\ \right\} \tag{1.9.5}$$

We can easily see that $\mathrm{G}_{v_i,0}\ \leq\ \mathrm{G}_{\mathfrak{B}_i,0}$. Let $\alpha\ \in\ \mathcal{O}_{v_i}$ then by Lemma 1.7.1 (iv) and

(v) $\alpha = a/b$ where $a,\ b \in \mathcal{O}_{\mathbb{K}}$ and $|b|_{v_i} = 1$. Let $\sigma \in \mathrm{G}_{\mathfrak{B}_i,0}$. Then

$$\begin{aligned}
\sigma(\alpha) - \alpha &= \frac{\sigma(a)}{\sigma(b)} - \frac{a}{b} \\
&= \frac{\sigma(a)\cdot b - \sigma(b)\cdot a}{b\cdot\sigma(b)} \\
&= \frac{(\sigma(a)-a)(\sigma(b)+b) + (ab - \sigma(ab))}{b\cdot\sigma(b)} \\
&\in \mathcal{M}_{v_i}
\end{aligned}$$

So that $\sigma \in \mathrm{G}_{v_i,0}$. We thus have the inclusion $\mathrm{G}_{\mathfrak{B}_i,0} \leq \mathrm{G}_{v_i,0}$ and consequently the equality

$$\mathrm{G}_{\mathfrak{B}_i,0} = \mathrm{G}_{v_i,0} \tag{1.9.6}$$

For $n \in \mathbb{N}$ we define the *$n-th$ ramification group of* v_i as

$$\mathrm{G}_{v_i,n} = \left\{ \sigma \in \mathrm{G} : \sigma(\alpha) - \alpha \in \mathcal{M}_{v_i}^{n+1} \text{ for all } \alpha \in \mathcal{O}_{v_i} \right\} \tag{1.9.7}$$

As in the case $n = 0$, it is easy to deduce that

$$\mathrm{G}_{\mathfrak{B}_i,n} = \mathrm{G}_{v_i,n} \text{ for all } n \in \mathbb{N} \text{ and } v_i \in \mathcal{A}_p \tag{1.9.8}$$

Let $\phi : \mathrm{Z}_{v_i} \longrightarrow \mathrm{G}_{v_i} = \mathrm{Aut}(\ \mathbb{F}_{v_i}\ /\ \mathbb{F}_p\ )$ be the natural projection homomorphism. If $g \in \mathrm{Z}_{v_i}$ is such that $\langle \phi(g) \rangle = Z_{v_i}$ then for all $\alpha \in \mathcal{O}_{v_i}$ and $s \in \mathbb{N}$ we have

$$g^s(\alpha) - \alpha^{p^s} \in \mathcal{M}_{v_i} \tag{1.9.9}$$

and we say that g acts as the *Frobenius automorphism on* $\mathbb{F}_{v_i}$. Theorem 1.8.1 can clearly be extended to Z_{v_i} and $\mathbb{F}_{v_i}$ by replacing $\mathfrak{B}_i$ with v_i.

Theorem 1.9.1. (Properties of Non-Archimedean Stabilizers) *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension,* $\mathrm{G} = \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$ and $p \in \mathbb{N}$ *a rational prime with ramification index* e *and residue class degree* f *in* $\mathbb{K}$. *Let* $\mathcal{A}_p = \{\ v_1,\ \ldots,\ v_t\ \}$ *(where* $t \in \mathbb{N}$ *) be the finite set of places of* $\mathbb{K}$ *that restrict to the* $p-$*adic place of* $\mathbb{Q}$.

Then

(i) G *acts transitively on* $\mathcal{A}_p$ *and for* v_i and $v_j \in \mathcal{A}_p$ and $g \in \mathrm{G}$ *such that* $g(v_i) = v_j$ *we have* $g\mathrm{Z}_{v_i}\ g^{-1} = \mathrm{Z}_{v_j}$,

(ii) *For all* $v_i \in \mathcal{A}_p$ *we have* $\left|\ \mathrm{G}_{v_i,0}\ \right| = e,\ \ \mathrm{Z}_{v_i}\ /\ \mathrm{G}_{v_i,0}$ *is cyclic of degree* f *and* $\mathrm{G}_{v_i} = \mathrm{Z}_{v_i}\ /\ \mathrm{G}_{v_i,0}$

(iii) $\mathrm{G}_{v_i,n} = \{\ 1\ \}$ *for sufficiently large* $n \in \mathbb{N}$,

(iv) *There exists an injective homomorphism*

$$\phi\ :\ \mathrm{G}_{v_i,0}\ /\ \mathrm{G}_{v_i,1} \longrightarrow \left(\ \mathcal{O}_{v_i}\ /\ \mathcal{M}_{v_i}\ \right)^{\times}$$

(v) *For all* $n \in \mathbb{N}$, *there exists an injective homomorphism*

$$\psi\ :\ \mathrm{G}_{v_i,n}\ /\ \mathrm{G}_{v_i,n+1} \longrightarrow \left(\ \mathcal{O}_{v_i}\ /\ \mathcal{M}_{v_i}\ \right)^{+}$$

From property (iv) we see that $\mathrm{G}_{v_i,0}\ /\ \mathrm{G}_{v_i,1}$ is a cyclic group whose order is a divisor of $p^f - 1$ and that $\mathrm{G}_{v_i,1}$ is the unique Sylow-p subgroup of $\mathrm{G}_{v_i,0}$. From property (v)

we see that $G_{v_i,n} \ / \ G_{v_i,n+1}$ is a finite abelian group of exponent p. From property (ii) and by considering the sequence

$$Z_{v_i} \ \supseteq \ G_{v_i,0} \ \supseteq \ G_{v_i,1} \ \supseteq \ \cdots \ \supseteq G_{v_i,m} \ = \ \{ \ 1 \ \} \tag{1.9.10}$$

we can see that the stabilizer Z_{v_i} is solvable.

Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension. Let $G = \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q} \ )$. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be a fixed embedding and let $\xi \in G$ correspond to complex conjugation with respect to η. Let $|| \cdot ||_\infty$ be the usual archimedean absolute value on $\mathbb{C}$. Then, from Theorem 1.5.2, $|| \cdot ||_\infty \circ \eta$ defines an archimedean absolute value on $\mathbb{K}$ and every archimedean absolute value on $\mathbb{K}$ is of this form. Let v be the place of $\mathbb{K}$ containing $|| \cdot ||_\infty \circ \eta$. As in the non-archimedean case define

$$Z_v \ \equiv \ \left\{ \ \sigma \in G \ : \ | \cdot |_{\sigma v} = | \cdot |_v \ \right\}$$

It is clear that $Z_v \ = \ \langle \xi \rangle$.

Chapter 2

The Absolute Weil Height

2.1 Definition

Let $\mathbb{E} \subset \mathbb{K}$ be finite extensions of $\mathbb{Q}$ and let u be a place of $\mathbb{E}$. Let $\mathcal{A}_u = \{ v_1, \ldots, v_t \}$ be the set of places of $\mathbb{K}$ that restrict to u on $\mathbb{E}$. For $\alpha \in \mathbb{K}$ we have by Theorems 1.5.1 and 1.5.2

$$[\mathbb{K} : \mathbb{E}] = \sum_{\mathcal{A}_u} [\mathbb{K}_v : \mathbb{E}_u], \tag{2.1.1}$$

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{E}}(\alpha) = \prod_{\mathcal{A}_u} \mathrm{Norm}_{\mathbb{K}_v/\mathbb{E}_u}(\alpha), \tag{2.1.2}$$

and

$$\left|\left| \alpha \right|\right|_v = \left|\left| \mathrm{Norm}_{\mathbb{K}_v/\mathbb{E}_u}(\alpha) \right|\right|_u^{1/[\mathbb{K}_v:\mathbb{E}_u]} \tag{2.1.3}$$

We note the following elementary identities

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{Q}] \tag{2.1.4}$$

$$[\mathbb{K}_v : \mathbb{Q}_u] = [\mathbb{K}_v : \mathbb{E}_u][\mathbb{E}_u : \mathbb{Q}_u] \tag{2.1.5}$$

which we use to derive the following

$$\begin{aligned}
|\alpha|_v &= \Big|\Big| \alpha \Big|\Big|_v^{[\mathbb{K}_v:\mathbb{Q}_u]/[\mathbb{K}:\mathbb{Q}]} \\
&= \Big|\Big| \operatorname{Norm}_{\mathbb{K}_v/\mathbb{E}_u}(\alpha) \Big|\Big|_u^{[\mathbb{K}_v:\mathbb{Q}_u]/[\mathbb{K}:\mathbb{Q}][\mathbb{K}_v:\mathbb{E}_u]} \\
&= \Big|\Big| \operatorname{Norm}_{\mathbb{K}_v/\mathbb{E}_u}(\alpha) \Big|\Big|_u^{[\mathbb{E}_u:\mathbb{Q}_u]/[\mathbb{K}:\mathbb{Q}]} \\
&= \Big| \operatorname{Norm}_{\mathbb{K}_v/\mathbb{E}_u}(\alpha) \Big|_u^{[\mathbb{E}_u:\mathbb{Q}_u][\mathbb{E}:\mathbb{Q}]/[\mathbb{K}:\mathbb{Q}][\mathbb{E}_u:\mathbb{Q}_u]} \\
&= \Big| \operatorname{Norm}_{\mathbb{K}_v/\mathbb{E}_u}(\alpha) \Big|_u^{1/[\mathbb{K}:\mathbb{E}]}
\end{aligned}$$

This last equality is equality (2.1.6).

By combining equations (2.1.2) and (2.1.6) we have

$$\prod_{\mathcal{A}_u} |\alpha|_v = \Big| \operatorname{Norm}_{\mathbb{K}/\mathbb{E}}(\alpha) \Big|_u^{1/[\mathbb{K}:\mathbb{E}]} \tag{2.1.7}$$

and in the case that $\alpha \in \mathbb{E}$

$$\prod_{\mathcal{A}_u} |\alpha|_v = |\alpha|_u \tag{2.1.8}$$

From equation (2.1.6) we can deduce that if $\alpha \in \mathbb{E}$ such that $|\alpha|_u < 1$ then for all $v \in \mathcal{A}_u$ we have $|\alpha|_v < 1$ and if $\alpha \in \mathbb{E}$ such that $|\alpha|_u > 1$ then for all $v \in \mathcal{A}_u$ we have $|\alpha|_v > 1$. From these remarks and equation (2.1.8) we can define the *absolute logarithmic Weil height*, $h : \overline{\mathbb{Q}}^\times \longrightarrow [0, \infty)$ as follows. Let $\alpha \in \overline{\mathbb{Q}}^\times$

and let $\mathbb{K}$ be any algebraic number field containing α then

$$h(\alpha) \;=\; \sum_{\mathcal{A}_{\mathbb{K}}} \log^{+} |\alpha|_v \tag{2.1.9}$$

2.2 Elementary Properties

Our first remark concerning the absolute Weil height is about its invariance with respect to Galois conjugation. Let β be a Galois conjugate of α. It then follows from Theorem 1.6.1 and equation (2.1.9) that

$$h(\alpha) \;=\; h(\beta) \tag{2.2.1}$$

The absolute Weil height is thus a function on the set of irreducible polynomials with coefficients in $\mathbb{Z}$. The following theorem was established by Kronecker [Kro57].

Theorem 2.2.1. (Kronecker) *Let* $\alpha \in \overline{\mathbb{Q}}^{\times}$. *Then*

$$h(\alpha) = 0 \quad \textit{if and only if} \quad \alpha \in \mathrm{Tor}(\,\overline{\mathbb{Q}}^{\times}\,) \tag{2.2.2}$$

Proof. Let $\alpha \in \overline{\mathbb{Q}}^{\times}$ be an algebraic number such that $h(\alpha) = 0$. Let $\{\, \alpha_1, \ldots, \alpha_d \,\}$ be the set of Galois conjugates of α. At every place v of $\mathbb{Q}(\alpha)$, we have $|\alpha|_v \leq 1$. From equation (1.7.2) we know that α is an algebraic integer. For $n \in \mathbb{N}$ let

$$f_n(x) \;=\; \prod_{i=1}^{d} (x - \alpha_i^n) \tag{2.2.3}$$

The coefficients of the $f_n(x)$ are symmetric functions of $\{\ \alpha_1,\ \ldots\ ,\ \alpha_d\ \}$ and consequently are rational integers bounded by the binomial coefficients $\binom{d}{i}$ for $i\ \in\ \{\ 0,\ \ldots\ ,\ d\ \}$. We define, for each $n \in \mathbb{N}$

$$\mathcal{F}_n\ =\ \{\ \alpha_i^n,\ \ldots\ ,\ \alpha_d^n\ \} \tag{2.2.4}$$

and we recognize that the set $\{\ \mathcal{F}_n\ :\ n\ \in\ \mathbb{N}\ \}$ is finite. Let $(b_n)_{n\in\mathbb{N}}$ be a sequence such that $f_{b_n}\ =\ f_{b_1}$. It follows that there exists $i,\ j\ \in\ \mathbb{N}$ such that $\alpha_1^{b_i}\ =\ \alpha_1^{b_j}$ where $b_j\ \neq\ b_i$. We consequently deduce that α_1 and consequently α is a root of unity. $\square$

We now describe the variatons on the absolute logarithmic Weil height with respect to raising nonzero algebraic numbers to rational powers. In the following, $||\cdot||_\infty$ will denote the usual archimedean absolute value on $\mathbb{C}$.

Lemma 2.2.2. (Height and Powers) *Let $\alpha\ \in\ \overline{\mathbb{Q}}^\times$ and $w\ \in\ \mathbb{Q}$. Then*

$$h(\ \alpha^w\ )\ =\ \big|\big|w\big|\big|_\infty\ \cdot\ h(\ \alpha\ )$$

Proof. By the Product Formula, Theorem 1.5.3, we have

$$0\ =\ \sum_{\mathcal{A}_{\mathbb{K}}} \log|\alpha|_v = \sum_{\mathcal{A}_{\mathbb{K}}} \log^+|\alpha|_v - \log^-|\alpha|_v \tag{2.2.5}$$

from which it follows

$$\sum_{\mathcal{A}_{\mathbb{K}}} \log^-|\alpha|_v\ =\ \sum_{\mathcal{A}_{\mathbb{K}}} \log^+|\alpha|_v \tag{2.2.6}$$

We note that

$$\sum_{\mathcal{A}_{\mathbb{K}}} \Big|\Big| \log |\alpha|_v \Big|\Big|_\infty \;=\; \sum_{\mathcal{A}_{\mathbb{K}}} \Big\{ \; \log^+ |\alpha|_v + \log^- |\alpha|_v \; \Big\} \tag{2.2.7}$$

and consequently

$$2 \cdot h(\alpha) \;=\; \sum_{\mathcal{A}_{\mathbb{K}}} \Big|\Big| \log |\alpha|_v \Big|\Big|_\infty \tag{2.2.8}$$

Using equation (2.2.8) we can deduce that for $w \in \mathbb{Q}$ and $\alpha \in \overline{\mathbb{Q}}^\times$ we have

$$h(\alpha^w) \;=\; \big|\big|w\big|\big|_\infty \cdot h(\alpha) \qquad \square \tag{2.2.9}$$

Lemma 2.2.3. (Galois Conjugates) *Let $\alpha,\ \beta \in \overline{\mathbb{Q}}^\times$ be Galois conjugates such that there exists $i,\ j \in \mathbb{N},\ \ i \neq j$ such that*

$$\alpha^i = \beta^j$$

Then $\alpha,\ \beta \in \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ )$.

Proof. By equations (2.2.1) and (2.2.9), this implies that $i \cdot h(\alpha) = j \cdot h(\alpha)$ and consequently that $h(\alpha) = 0$. By Theorem 2.2.1, $\alpha \in \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ )$. $\square$

Lemma 2.2.4. (Sums and Products) *Let $t \in \mathbb{N}$ and $\alpha_1,\ \ldots,\ \alpha_t \in \overline{\mathbb{Q}}^\times$ then*

$$h\Bigg(\prod_{i=1}^{t} \alpha_i \Bigg) \;\leq\; \sum_{i=1}^{t} h(\alpha_i) \tag{2.2.10}$$

and

$$h\left(\sum_{i=1}^{t} \alpha_i \right) \leq t \cdot \sum_{i=1}^{t} h(\alpha_i) \tag{2.2.11}$$

Proof. Let $\mathbb{K} \equiv \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$. As before, let $\mathcal{A}_{\mathbb{K}}$ be the set of places of $\mathbb{K}$. For all but finitely many $v \in \mathcal{A}_{\mathbb{K}}$ we have $|\alpha_i|_v = 1$ for all $i \in \{ 1, \ldots, t \}$. We can consequently deduce, using equality (2.1.9) that

$$\begin{aligned}
\prod_{\mathcal{A}_{\mathbb{K}}} \max\left\{ 1, \left| \prod_{i=1}^{t} \alpha_i \right|_v \right\} &\leq \prod_{\mathcal{A}_{\mathbb{K}}} \prod_{i=1}^{t} \max\left\{ 1, |\alpha_i|_v \right\} \\
&= \prod_{i=1}^{t} \prod_{\mathcal{A}_{\mathbb{K}}} \max\left\{ 1, |\alpha_i|_v \right\} \\
&= \prod_{i=1}^{t} e^{h(\alpha_i)}
\end{aligned}$$

from which we obtain inequality (2.2.10)

For $v \in \mathcal{A}_{\mathbb{K}}$ non-archimedean we have, from the strong triangle inequality, inequality (1.1.1), that

$$\begin{aligned}
\max\left\{ 1, \left| \sum_{i=1}^{t} \alpha_i \right|_v \right\} &\leq \max\left\{ 1, \max\{ |\alpha_i|_v : 1 \leq i \leq t \} \right\} \\
&\leq \prod_{i=1}^{t} \max\left\{ 1, |\alpha_i|_v \right\}
\end{aligned}$$

and hence that

$$\prod_{v \nmid \infty} \max\left\{ 1, \left| \sum_{i=1}^{t} \alpha_i \right|_v \right\} \leq \prod_{v \nmid \infty} \prod_{i=1}^{t} \max\left\{ 1, |\alpha_i|_v \right\}$$

Since for all but finitely many $v \in \mathcal{A}_{\mathbb{K}}$ we have $|\alpha_i|_v = 1$ for all $i \in \{ 1, \ldots, t \}$, we can interchange the order of products and obtain

$$\prod_{v \nmid \infty} \max\left\{ 1, \left| \sum_{i=1}^{t} \alpha_i \right|_v \right\} \leq \prod_{i=1}^{t} \prod_{v \nmid \infty} \max\left\{ 1, |\alpha_i|_v \right\}$$

For $v \in \mathcal{A}_{\mathbb{K}}$ archimedean we have, from the ordinary triangle inequality, that

$$\begin{aligned} \max\left\{ 1, \left\| \sum_{i=1}^{t} \alpha_i \right\|_v \right\} &\leq \max\left\{ 1, \sum_{i=1}^{t} ||\alpha_i||_v \right\} \\ &\leq t \cdot \prod_{i=1}^{t} \max\left\{ 1, ||\alpha_i||_v \right\} \end{aligned}$$

By equations (1.5.0) and (1.5.2) we can further deduce that

$$\begin{aligned} \max\left\{ 1, \left| \sum_{i=1}^{t} \alpha_i \right|_v \right\} &\leq t^{[\mathbb{K}_v:\mathbb{Q}_v]/[\mathbb{K}:\mathbb{Q}]} \cdot \prod_{i=1}^{t} \max\left\{ 1, |\alpha_i|_v \right\} \\ \prod_{v \mid \infty} \max\left\{ 1, \left| \sum_{i=1}^{t} \alpha_i \right|_v \right\} &\leq t \cdot \prod_{v \mid \infty} \prod_{i=1}^{t} \max\left\{ 1, |\alpha_i|_v \right\} \\ \prod_{v \mid \infty} \max\left\{ 1, \left| \sum_{i=1}^{t} \alpha_i \right|_v \right\} &\leq t \cdot \prod_{i=1}^{t} \prod_{v \mid \infty} \max\left\{ 1, |\alpha_i|_v \right\} \end{aligned}$$

from which the proof of inequality (2.2.11) is now complete. $\square$.

Let $\zeta_m \in \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$. It follows from equation (2.1.9) that

$$h(\alpha) \ = \ h\big(\ \zeta_m \cdot \alpha\ \big) \tag{2.2.12}$$

The logarithmic absolute Weil height is thus a function on the quotient group $\overline{\mathbb{Q}}^{\times}\ /\ \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$.

Lemma 2.2.5. (The Height as a Metric) *Let* $\mathcal{Q} \ \equiv \ \overline{\mathbb{Q}}^{\times}\ /\ \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$ *and define*

$$d: \ \mathcal{Q} \times \mathcal{Q} \longrightarrow [0, \infty)$$

by

$$d\big(\ \alpha,\ \beta\ \big) \ = \ h\big(\ \alpha \cdot \beta^{-1}\ \big)$$

Then d *is a metric on* $\mathcal{Q}$.

Proof. Let $\alpha, \beta,$ and $\gamma \in \mathcal{Q}$. Suppose that $d(\alpha, \beta) = 0$ then $h(\alpha \cdot \beta^{-1}) = 0$. From Theorem 2.2.1, $\alpha \cdot \beta^{-1} = 1$ or equivalently $\alpha = \beta$. Since $\mathcal{Q}$ is abelian, we have, using equation 2.2.9, that $d(\alpha, \beta) = d(\beta, \alpha)$. It is clear that $d(\alpha, \beta) = d(\alpha \cdot \gamma, \gamma \cdot \beta)$ and from Lemma 2.2.4 that $d(\alpha \cdot \gamma, \gamma \cdot \beta) \leq d(\alpha, \gamma) + d(\gamma, \beta)$. $\square$

It is known that $(\mathcal{Q}, d)$ is not complete (Vaaler [Val07]). Let $\mathcal{G}$ denote the completion of $(\mathcal{Q}, d)$. Allcock Vaaler [Val07] has recently studied $\mathcal{G}$ and identified fundamental properties of this complete metric space.

2.3 Lower Bounds for the Height

In this section, we describe several results providing lower bounds on the Weil height of algebraic numbers different from zero and the roots of unity. Part of this thesis is about such bounds. The establishment of upper bounds for the Weil height of algebraic numbers is a separate area of research.

In this section, $||\cdot||_\infty$ will denote the usual archimedean absolute value on $\mathbb{C}$. For an algebraic number field $\mathbb{K}$, we let $\mathcal{A}_{\mathbb{K},\infty}$ be the set of archimedean places of $\mathbb{K}$. For $\mathbb{K}$ a finite Galois extension of $\mathbb{Q}$ let

$$\mathcal{U}_{\mathbb{K},\infty} \equiv \left\{ \alpha \in \mathbb{K} \ : \ |\alpha|_v = 1 \quad \forall\, v \in \mathcal{A}_{\mathbb{K},\infty} \right\}$$

Let $\mathcal{U}_\infty \equiv \bigcup_{\mathbb{K}} \mathcal{U}_{\mathbb{K},\infty}$, where the union is over all finite Galois extensions of $\mathbb{Q}$. We have that $\mathcal{U}_\infty$ is a multiplicative group, $\mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ ) \trianglelefteq \mathcal{U}_\infty$ and

$$h : \left(\mathcal{U}_\infty \ / \ \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ ) \right) \longrightarrow [0, \infty)$$

is well defined. The following theorem is a special case of a more general result due to Schinzel, Corollary 1 of [Sch73] applied to the polynomial $P(z) = z - \alpha$ and $\alpha \notin \mathcal{U}_\infty$.

Theorem 2.3.1. (Schinzel) *Let α be a nonzero algebraic integer, $\alpha \notin \mathcal{U}_\infty$. If $\mathbb{Q}(\alpha)$ is totally real or is a totally complex quadratic extension of a totally real field. Then*

$$h(\alpha) \ \geq \ \frac{1}{2} \cdot \log\left(\ \frac{1+\sqrt{5}}{2} \ \right) \tag{2.3.1}$$

with equality only in the case $\pm\ \alpha$ a root of $x^2 - x - 1$ or $x^2 + x - 1$.

We note that the proofs of Schinzel's more general results are lengthy and that G. Hoehn and N.P. Skoruppa [Hoe93] have provided a one page proof of inequality (2.3.1) for the case α totally real.

Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with $G \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Suppose that G is Abelian. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in G$ correspond to complex conjugation with respect to η. Let $\mathbb{F}_{\langle \xi \rangle}$ be the subfield of $\mathbb{K}$ fixed by ξ. Let $\alpha \in \mathbb{K}^{\times}$ and $\alpha \notin \mathcal{U}_{\infty}$ be not real under η. Then $\mathbb{Q}(\alpha)$ is a totally complex quadratic extension of the totally real field $\mathbb{Q}(\alpha) \bigcap \mathbb{F}_{\langle \xi \rangle}$. It then follows from Theorem 2.3.1 that

$$h(\alpha) \geq \frac{1}{2} \cdot \log\left(\frac{1+\sqrt{5}}{2} \right)$$

F. Amoroso and R. Dvornicich expanded on this observation by analyzing $\mathcal{U}_{\infty,\mathbb{K}}$. In [Am00a] they were able to establish the following.

Theorem 2.3.2. (Amoroso and Dvornicich) *Let $m \in \mathbb{N}$ and let ζ_m be a primitive $m-$th root of unity. Let $\mathbb{K} = \mathbb{Q}(\zeta_m)$. For $\alpha \in \mathbb{K}^{\times} - \mathrm{Tor}(\ \mathbb{K}^{\times}\ )$,*

$$h(\alpha) \geq \begin{cases} \frac{1}{8} \cdot \log\left(\frac{7}{2} \right), & \text{if} \quad 7 \nmid m; \\ \frac{1}{6} \cdot \log\left(\frac{5}{2} \right), & \text{if} \quad 7 \mid m \text{ and } 5 \nmid m; \\ \frac{1}{12} \cdot \log\left(\frac{11}{2} \right), & \text{if} \quad 35 \mid m \text{ and } 11 \nmid m; \\ \frac{1}{12} \cdot \log\left(5 \right), & \text{if} \quad 385 \mid m. \end{cases}$$

and if $4 \mid m$ and there is no root of unity $\zeta \in \mathbb{K}$ such that $\alpha \cdot \zeta$ is contained in a

proper cyclotomic subextension of $\mathbb{K}$*, then*

$$h(\alpha) \ \geq \ \frac{1}{4} \cdot \log 2$$

The Kronecker-Weber Theorem (see page 200 of [Koc00]) states that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$ and hence the Theorem of Amoroso and Dvornicich covers all algebraic numbers (different from zero and the roots of unity) contained in abelian extensions of $\mathbb{Q}$.

Each of the lower bounds in Theorem 2.3.2 is less than the lower bound of inequality (2.3.1) and the lowest is $\frac{1}{12} \cdot \log 5$. Amoroso and Dvornicich point out that this number is not known to be the smallest possible and identify $\frac{1}{12} \cdot \log 7$ as their lowest known abelian height. We thus propose the following research problem.

Research Problem 1. What is the smallest positive Abelian height?

As a special case of a more general result, S. Zhang [Zha92] proved the following

Theorem 2.3.3. (Zhang) *Let* α *be an algebraic number different from 0, 1 and the primitive sixth roots of unity. Then there exists an absolute constant* $C > 0$ *such that*

$$h(\alpha) + h(1 - \alpha) \ \geq \ C \tag{2.3.2}$$

D. Zagier [Zag93] found the best possible C, provided an elementary proof of the inequality (2.3.2), and identified all cases of equality.

Theorem 2.3.4. (Zagier) *For all algebraic numbers* $\alpha \neq 0,\ 1,\ (1 \pm \sqrt{-3})/2$ *we have*

$$h(\alpha) + h(1-\alpha) \ \geq \ \frac{1}{2} \cdot \log\left(\ \frac{1+\sqrt{5}}{2} \ \right) \tag{2.3.3}$$

with equality if and only if α *or* $1-\alpha$ *is a primitive* 10*-th root of unity.*

As a corollary (Corollary 2.1 of [Beu97]) of a more general theorem, F. Beukers and D. Zagier generalized Theorem 2.3.4 with the following result.

Theorem 2.3.5. (Beukers and Zagier) *Let* $N \in \mathbb{Z}$ *and let* $\alpha_1,\ \ldots,\ \alpha_r \in \overline{\mathbb{Q}}^{\times}$ *be such that*

$$\sum_{i=1}^{r} \alpha_i \ = \ N \ \neq \ \sum_{i=1}^{r} \frac{1}{\alpha_i} \tag{2.3.4}$$

then

$$\sum_{i=1}^{r} h(\alpha_i) \ \geq \ \frac{1}{2} \cdot \log\left(\ \frac{1+\sqrt{5}}{2} \ \right) \tag{2.3.5}$$

Since the equation

$$\alpha + (1-\alpha) \ = \ \frac{1}{\alpha} + \frac{1}{1-\alpha} \tag{2.3.6}$$

implies that α is a primitive sixth root of unity, we see that this new result strictly contains inequality (2.3.3). Beukers and Zagier note that for $r \geq 4$ equality is attained in inequality (2.3.5) for $\alpha_1 = -\zeta_5,\ \alpha_2 = 1 + \zeta_5,\ \alpha_3 = \zeta_{r-2},\ \ldots,\ \alpha_r = \zeta_{r-2}^{r-3}$.

Recently, C. Samuels [Sam06] has extended Theorem 2.3.5 by allowing N to be a totally real algebraic integer. By letting α be totally real and different from ± 1 his new result recovers inequality 2.3.1.

Theorem 2.3.6. (Samuels) *Let N be a totally real algebraic integer and let $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}^{\times}$ be such that*

$$\sum_{i=1}^{r} \alpha_i \;=\; N \;\neq\; \sum_{i=1}^{r} \frac{1}{\alpha_i} \tag{2.3.7}$$

then

$$\sum_{i=1}^{r} h(\alpha_i) \;\geq\; \frac{1}{2} \cdot \log\left(\frac{1+\sqrt{5}}{2} \right) \tag{2.3.8}$$

It is worth mentioning that P.E. Blanskby and H.L. Montgomery [Bla71] considered a similar problem and established the following.

Theorem 2.3.7. (Blanksby and Montgomery) *Let $s, n \in \mathbb{N}$. Let α be an algebraic integer of degree $n > 1$. Let $\alpha_1, \ldots, \alpha_n$ be the distint Galois conjugates of α and let $\overline{|\alpha|} = \max\limits_{1 \leq i \leq n} ||\alpha_i||_{\infty}$. Suppose that α has $2 \cdot s$ non real Galois conjugates and at least one real Galois conjugate. Then*

$$\overline{|\alpha|} > 1 + \frac{\log(s+2)}{16 \cdot (s+2)^2} \tag{2.3.9}$$

We conclude this section by reporting a work of G.P. Dresden [Dre98]. He was able to extend Theorem 2.3.4 with the following

Theorem 2.3.8. (Dresden) *Let α be an algebraic number different from 0 and 1.*

(i) *For a primitive six root of unity,*

$$h(\alpha) + h\left(\frac{1}{1-\alpha} \right) + h\left(1 - \frac{1}{\alpha} \right) = 0 \tag{2.3.10}$$

(ii) *Otherwise,*

$$h(\alpha) + h\left(\frac{1}{1-\alpha} \right) + h\left(1 - \frac{1}{\alpha} \right) \geq 0.4218..... \tag{2.3.11}$$

with equality for α any root of

$$\begin{aligned} P(z) &= z^6 - 3z^5 + 5z^4 - 5z^3 - 3z + 1 \\ &= (z^2 - z + 1)^3 - (z^2 - z)^2 \end{aligned}$$

In the next section, we will make a contribution to these types of results and pose a natural research problem concerning the work of Samuels, Zagier and Beukers.

2.4 The Height of Complex Conjugation

The following observation was made in 2007 and is a generalization of Theorem 2.3.1.

Theorem 2.4.1. (Garza) *Let $\alpha \in \overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\overline{\mathbb{Q}}^{\times})$. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding. Let Λ be the set of Galois conjugates of α that are real with respect to η. Suppose that $|\Lambda| \neq 0$. Let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$*

and let $R_\alpha \equiv |\Lambda|/d$. *Let* $\beta = 1 - 1/R_\alpha$. *Then*

$$h(\alpha) \;\geq\; \log\left(\frac{2^\beta + \sqrt{4^\beta + 4}}{2} \right)^{R_\alpha/2} \tag{2.4.1}$$

Proof. Let $||\cdot||_\infty$ be the usual archimedean absolute value on $\mathbb{C}$. Let $\delta \equiv 1 - \alpha^2$. For each place v of $\mathbb{K}$ define

$$b_v \;\equiv\; \frac{\left|\left|\; \delta \;\right|\right|_v}{\max\left\{\; 1,\; ||\alpha||_v^2 \;\right\}}$$

By the ultrametic inequality, for each $v \nmid \infty$ we have that $b_v \leq 1$.

For each $\gamma \in \Lambda$ define

$$a_\gamma \;\equiv\; \frac{\left|\left|1 - \gamma^2\right|\right|_\infty}{\max\left\{\; 1,\; ||\gamma||_\infty^2 \;\right\}}$$

For $\gamma \in \Lambda$ such that $||\gamma||_\infty > 1$ we have

$$a_\gamma = \left|\left|1 - \frac{1}{\gamma^2}\right|\right|_\infty$$

For $\gamma \in \Lambda$ such that $||\gamma||_\infty < 1$ we have

$$a_\gamma = \left|\left|1 - \gamma^2\right|\right|_\infty$$

For $\gamma \in \Lambda$ such that $||\gamma||_\infty > 1$ we define $\gamma^{'} = 1/\gamma$ and for $\gamma \in \Lambda$ such that $||\gamma||_\infty < 1$ we define $\gamma^{'} = \gamma$. We thus have, by Lemma 2.2.2 with $w = -1$, that

$$\prod_{\gamma \in \Lambda} \left(\gamma^{'}\right)^2 \ \geq \ \frac{1}{(e^{d \cdot h(\alpha)})^4}$$

Using the Arithmetic-Goemetric Mean Inequality twice we have

$$\begin{aligned}
\prod_{\gamma \in \Lambda} (1 - (\gamma^{'})^2) \ &\leq \ \left(\frac{1}{|\Lambda|} \left(\sum_{\gamma \in \Lambda} (1 - (\gamma^{'})^2) \right) \right)^{|\Lambda|} \\
&= \ \left(1 - \frac{1}{|\Lambda|} \sum_{\gamma \in \mathfrak{I}} (\gamma^{'})^2 \right)^{|\Lambda|} \\
&\leq \ \left(1 - \left(\prod_{\gamma \in \Lambda} (\gamma^{'})^2 \right)^{1/|\Lambda|} \right)^{|\Lambda|} \\
&\leq \ \left(1 - \left(\frac{1}{(e^{d \cdot h(\alpha)})^4} \right)^{1/dR_\alpha} \right)^{dR_\alpha}
\end{aligned}$$

By the triangle inequality, $\forall \ v \mid \infty$ we have $b_v \leq 2$. Let $\mathcal{A}_{\mathbb{K}}$ be the set of places of $\mathbb{K}$ and define

$$B \ \equiv \ \prod_{\mathcal{A}_{\mathbb{K}}} {b_v}^{(d_v/d)}$$

From equation (2.1.1), $\sum\limits_{v \mid \infty} d_v = d$ and from the Galois action on places

$$B \leq 2^{1-R_\alpha} \cdot \left(1 - \left(\frac{1}{(e^{d \cdot h(\alpha)})^4} \right)^{1/dR_\alpha} \right)^{R_\alpha}$$

If $d \cdot R_\alpha = |\Lambda|$ is sufficiently large in comparison to $e^{d \cdot h(\alpha)}$ it follows that $B < 1$.

Fix v. Since

$$||\delta||_v \;=\; \big|\delta\big|_v^{d/d_v} \;=\; b_v \cdot \max\Big\{\; 1,\; ||\alpha||_v^2 \;\Big\}$$

we have

$$\log|\delta|_v \;=\; \left(\;\frac{d_v}{d}\;\right)\cdot\left(\;\log b_v + 2\cdot\log^+||\alpha||_v\;\right)$$

Summing over all places and using the Product Formula

$$\begin{aligned} 0 &= \sum_v \log|\delta|_v \\ 0 &= \sum_v \log b_v^{(d_v/d)} + 2\cdot\sum_v \log^+|\alpha|_v \\ 0 &= \log B + 2\cdot h(\alpha) \end{aligned}$$

We thus have

$$\begin{aligned} h(\alpha) &= \frac{1}{2}\cdot\log\left(\frac{1}{B}\right) \\ h(\alpha) &\geq \frac{1}{2}\cdot\log\left(2^{R_\alpha-1}\cdot\left(1-\left(\frac{1}{(e^{d\cdot h(\alpha)})^4}\right)^{1/dR_\alpha}\right)^{-R_\alpha}\right) \\ d\cdot h(\alpha) &\geq \frac{d}{2}\cdot\log\left(2^{R_\alpha-1}\cdot\left(1-\left(\frac{1}{(e^{d\cdot h(\alpha)})^4}\right)^{1/dR_\alpha}\right)^{-R_\alpha}\right) \\ d\cdot h(\alpha) &\geq \log\left(2^{R_\alpha-1}\cdot\left(1-\left(\frac{1}{(e^{d\cdot h(\alpha)})^4}\right)^{1/dR_\alpha}\right)^{-R_\alpha}\right)^{d/2} \end{aligned}$$

We notice that for a fixed d and R_α, if $h(\alpha)$ decreases the right hand side of the inequality increases. As a result, the inequality implies a lower bound on $h(\alpha)$. We deduce as follows

$$\begin{aligned}
e^{d\cdot h(\alpha)} &\geq \left(2^{R_\alpha - 1}\cdot\left(1-\left(\frac{1}{(e^{d\cdot h(\alpha)})^4}\right)^{1/dR_\alpha}\right)^{-R_\alpha}\right)^{d/2} \\
(e^{d\cdot h(\alpha)})^{2/d} &\geq 2^{R_\alpha-1}\cdot\left(\frac{(e^{d\cdot h(\alpha)})^{4/dR_\alpha}}{(e^{d\cdot h(\alpha)})^{4/dR_\alpha}-1}\right)^{R_\alpha} \\
(e^{d\cdot h(\alpha)})^{2/dR_\alpha} &\geq 2^\beta\cdot\frac{(e^{d\cdot h(\alpha)})^{4/dR_\alpha}}{(e^{d\cdot h(\alpha)})^{4/dR_\alpha}-1} \\
1 &\geq 2^\beta\cdot\frac{(e^{d\cdot h(\alpha)})^{2/dR_\alpha}}{(e^{d\cdot h(\alpha)})^{4/dR_\alpha}-1} \\
(e^{d\cdot h(\alpha)})^{4/dR_\alpha}-1 &\geq 2^\beta\cdot(e^{d\cdot h(\alpha)})^{2/dR_\alpha} \\
(e^{d\cdot h(\alpha)})^{4/dR_\alpha}-2^\beta\cdot(e^{d\cdot h(\alpha)})^{2/dR_\alpha}-1 &\geq 0
\end{aligned}$$

From the quadratic formula,

$$e^{d\cdot h(\alpha)} \geq \left(\ \frac{2^\beta+\sqrt{4^\beta+4}}{2}\ \right)^{dR_\alpha}$$

□

We are able to establish the following theorem which applies to all nonzero algebraic numbers outside the multiplicave group $\mathcal{U}_\infty$.

Theorem 2.4.2. **(Garza)** *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension of finite degree. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $\alpha \in \mathbb{K}^\times - \mathcal{U}_{\infty,\mathbb{K}}$. Let $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding. Let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to σ. Let*

$\mathrm{Z_G}(\xi) = \{\ x \in \mathrm{G} : x\xi = \xi x\ \}$. *Let* $n = [\mathrm{G} : \mathrm{Z_G}(\xi)]$. *Then*

$$h(\alpha) \geq \log\left(\frac{2^{1-n} + \sqrt{4^{1-n}+4}}{2} \right)^{1/(2\cdot n)} \tag{2.4.2}$$

Proof. If, with respect to σ, α does not have a real Galois conjugate let $\gamma \equiv \alpha \cdot \xi(\alpha)$ and if α has a real Galois conjugate, τ, let $\gamma = \tau^2$. Since $\alpha \notin \mathcal{U}_\infty$ we can assume that $\gamma > 1$. Let $\mathrm{H}_{\mathbb{Q}(\gamma)}$ denote the subgroup of G that fixes the field $\mathbb{Q}(\gamma)$. Let $\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\gamma)}) = \{\ x \in \mathrm{G}\ :\ x\mathrm{H}_{\mathbb{Q}(\gamma)}x^{-1} = \mathrm{H}_{\mathbb{Q}(\gamma)}\ \}$. From Galois theory we recall that $[\mathrm{G} : \mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\gamma)})]$ is the number of subfields of $\mathbb{K}$ that are distinct from and conjugate to $\mathbb{Q}(\gamma)$.

$$\begin{aligned} \left| \frac{\mathrm{Z_G}(\xi)}{\mathrm{Z_G}(\xi) \bigcap \mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\gamma)})} \right| &\geq \frac{|\mathrm{Z_G}(\xi)|}{|\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\gamma)})|} \\ &= \frac{1}{n} \cdot \frac{|\mathrm{G}|}{|\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\gamma)})|} \end{aligned}$$

Consequently, at least $1/n$ of the elements of the orbit of $\mathbb{Q}(\gamma)$ under $\mathrm{G}/\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\gamma)})$ are the images of $\mathbb{Q}(\gamma)$ by elements of $\mathrm{Z_G}(\xi)$ so that at least $1/n$ of the Galois conjugates of γ are real and positive under σ. It then follows as in the proof of Theorem 2.3.1 but with $\delta = 1 - \gamma$ instead of $\delta = 1 - \alpha^2$ that

$$h(\alpha) \geq \log\left(\frac{2^{1-n} + \sqrt{4^{1-n}+4}}{2} \right)^{1/(2\cdot n)} \quad \square$$

Suppose that $\alpha \in \mathcal{U}_\infty$ and let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$. Let $\alpha_1, \ldots, \alpha_d$ be the distinct Galois conjugates of α and let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$.

Let $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ be a fixed embedding of $\mathbb{K}$ into $\mathbb{C}$. Let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to σ. Then, since $\alpha \in \mathcal{U}_\infty$ we have $\xi(\alpha_i) = 1/\alpha_i$ for $1 \leq i \leq d$. From this, we conclude that $\xi \in \mathrm{Z_G}$. We can thus formulate the following corollary to Theorem 2.4.1 which does not mention the exceptional numbers, $\mathcal{U}_\infty$.

Corollary 2.4.3. (Garza) *Let $\alpha \in \overline{\mathbb{Q}}^\times - \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ )$. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$ and let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Suppose that $|\mathrm{Z_G}|$ is odd. Let $[\mathrm{G} : \mathrm{Z_G}] = n$. Then*

$$h(\alpha) \geq \log\left(\frac{2^{1-n} + \sqrt{4^{1-n}+4}}{2} \right)^{1/(2\cdot n)}$$

Similar to the manner in which Amoroso and Dvornicich [Am00a] extended the work of Schinzel [Sch73] by analyzing the multiplicative group $\mathcal{U}_\infty$ / Tor($\overline{\mathbb{Q}}^\times$) we suggest a new research effort to extend our Theorem 2.4.1 to cover the exceptional group $\mathcal{U}_\infty$ / Tor($\overline{\mathbb{Q}}^\times$).

Reasearch Problem 2. Study the group $\mathcal{U}_\infty$ / Tor($\overline{\mathbb{Q}}^\times$) and extend Corollary 2.4.3 in the same manner that Amoroso and Dvornicich [Am00a] **extended the result of Schinzel** [Sch73].

We now revisit the result of C. Samuels [Sam06], F. Beukers and D. Zagier [Beu97] and propose the following.

Research Problem 3. Let N be an algebraic integer. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(N)$. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding. Let Λ be the set of Galois conjugates of N that are real under η. Suppose that $|\Lambda| \neq 0$. Define

$R_N \equiv |\Lambda|/[\mathbb{Q}(N):\mathbb{Q}]$ **and** $\beta \equiv 1 - 1/R_\alpha$**. Let** $\alpha_1, \ \ldots \ , \ \alpha_r \ \in \ \overline{\mathbb{Q}}^\times$**. If**

$$\alpha_1 + \cdots + \alpha_r \ = \ N \ \neq \frac{1}{\alpha_1} + \cdots + \frac{1}{\alpha_1} + \cdots + \frac{1}{\alpha_r}$$

Is it true that

$$\sum_{i=1}^{r} h(\alpha_i) \ \geq \ \log\left(\ \frac{2^\beta + \sqrt{4^\beta + 4}}{2} \ \right)^{R_N/2}$$

?

2.5 Non-Archimedean Estimates

Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension. In this section we use non-archimedean places to translate information about $G \equiv \text{Aut}(\mathbb{K}/\mathbb{Q})$ into lower bounds on the height of $\alpha \in \mathbb{K}^\times - \text{Tor}(\mathbb{K}^\times)$. Unlike the previous section where $\mathcal{U}_\infty$ was exceptional, the non-archimedean methods do not distiguish between $\alpha \in \mathcal{U}_\infty$ and $\alpha \notin \mathcal{U}_\infty$. We will use the structure of the stabilizer of a non-archimedean place as presented in Section 1.9. Similar and related results can be found in [Mig78], [Am00b] and [Bom02].

Lemma 2.5.1. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension and let $p \in \mathbb{N}$ be a rational prime with ramification index e in $\mathbb{K}$. Let $\mathcal{A}_p = \{ v_1, \ldots, v_t \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$* extending the *p-adic place of $\mathbb{Q}$. For $v_i \in \mathcal{A}_p$ let $\mathcal{M}_{v_i} = \{ \alpha \in \mathbb{K} : |\alpha|_{v_i} < 1 \}$. Let $s \in \mathbb{N}$ and $s \leq t$. Let $\beta \in \mathbb{K}^\times$ and $a_1, \ldots, a_s \in \mathbb{N} \bigcup \{ 0 \}$ such that $\beta \in \bigcap_{i=1}^{s} \mathcal{M}_{v_i}^{a_i}$. Then*

$$\sum_{\mathcal{A}_p} \log^- |\beta|_{v_i} \geq \left(\log p \right) \cdot \left(\frac{1}{e \cdot t} \right) \cdot \left(\sum_{i=1}^{s} a_i \right) \tag{2.5.1}$$

Proof. Let $\mathfrak{B}_i = \mathcal{M}_{v_i} \bigcap \mathcal{O}_\mathbb{K}$ and let $\nu_{\mathfrak{B}_i} : \mathcal{O}_\mathbb{K} \longrightarrow \mathbb{N} \bigcup \{ 0 \}$ be the valuation on $\mathcal{O}_\mathbb{K}$ associated to $\mathfrak{B}_i$ as defined by equation (1.7.4). From Theorem 1.1.1 and Section 1.4, for each $\phi \in v_i$ there exists $\rho \in (0,1)$ such that for all $\gamma \in \mathbb{K}^\times$, $\phi(\gamma) = \rho^{-\nu_{\mathfrak{B}_i}(\gamma)}$. Since $\nu_{\mathfrak{B}_i}(p) = e$ and $||p||_{v_i} = p^{-1}$, the ρ associated to $||\cdot||_{v_i}$ is $p^{-1/e}$. Since $\mathbb{K}/\mathbb{Q}$ is Galois, the local degrees of each place in $\mathcal{A}_p$ are equal. By Theorem 1.5.1, their

sum is $[\mathbb{K} : \mathbb{Q}]$ so that the ρ associated to $|\cdot|_{v_i}$ is $p^{-1/et}$. Let π_i be a uniformizing parameter for $\mathcal{M}_{v_i}$. Then $\nu_{\mathfrak{B}_i}(\pi_i) = 1$ and $|\pi_i|_{v_i} = p^{-1/et}$. It follows that

$$\sum_{\mathcal{A}_p} \log^- |\beta|_{v_i} \geq \left(\log p \right) \cdot \left(\frac{1}{e \cdot t} \right) \cdot \left(\sum_{i=1}^{s} a_i \right) \quad \square$$

Lemma 2.5.2. *Let $m,\ n \in \mathbb{N}$. Let $\omega \in \overline{\mathbb{Q}}^{\times}$ and let $d = [\mathbb{Q}(\omega) : \mathbb{Q}]$. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\omega)$. Let $\omega_1, \ldots, \omega_n$ be n distinct Galois conjugates of ω. For each $k \in \{ 1, \ldots, m \}$ and $j \in \{ 1, \ldots, n \}$ let $c_k \in \mathbb{Z} - \{ 0 \}$, $\zeta_k \in \mathrm{Tor}(\overline{\mathbb{Q}}^{\times})$ and $b_{j,k} \in \mathbb{N} \bigcup \{ 0 \}$ such that $\sum_{j=1}^{n} \sum_{k=1}^{m} b_{j,k} \geq 1$. Define*

$$\delta \equiv \sum_{k=1}^{m} c_k \zeta_k \prod_{j=1}^{n} \omega_j^{(b_{j,k})}$$

$$M_j \equiv \max\left\{ b_{j,k} \;\middle|\; 1 \leq k \leq m \right\}$$

$$M \equiv \sum_{j=1}^{n} M_j$$

$$L \equiv \sum_{k=1}^{m} |c_k|$$

For each archimedean place v of $\mathbb{K}$, define a_v by

$$a_v \equiv \frac{\left|\left|\ \delta\ \right|\right|_v}{\prod_{j=1}^{n} \max\left\{ 1,\ \left|\left| \omega_j^{M_j} \right|\right|_v \right\}}$$

let

$$A \equiv \prod_{v \mid \infty} a_v{}^{(d_v/d)}$$

For each non-archimedean place v of $\mathbb{K}$, define b_v by

$$b_v \;\equiv\; \frac{\left|\left|\;\delta\;\right|\right|_v}{\prod_{j=1}^{n} \max\left\{\;1,\;\left|\left|\omega_j^{M_j}\right|\right|_v\;\right\}}$$

let

$$B \;\equiv\; \prod_{v\,\nmid\,\infty} {b_v}^{(d_v/d)}$$

If $\delta \neq 0$, then $B \;\leq\; 1,\;\; A \;\leq\; L,\; B \cdot A \;\leq\; 1,\;\;$ and

$$M \cdot h(\omega) \;=\; -\log(\;A \cdot B\;)$$

Proof. For each archimedean place v,

$$\log ||\delta||_v \;=\; \frac{d}{d_v} \cdot \log |\delta|_v$$

it follows that

$$\begin{aligned} \log |\delta|_v \;&=\; \left(\;\frac{d_v}{d}\;\right) \cdot \left(\;\log a_v + \sum_{j=1}^{n} \log^+ \left|\left|\omega_j^{M_j}\right|\right|_v\;\right) \\ &=\; \log {a_v}^{(d_v/d)} + \sum_{j=1}^{n} M_j \log^+ |\omega|_v \end{aligned}$$

For each non-archimedean place v,

$$\log ||\delta||_v \;=\; \frac{d}{d_v} \cdot \log |\delta|_v$$

it follows that

$$\begin{aligned}\log|\delta|_v &= \left(\frac{d_v}{d}\right)\cdot\left(\log b_v + \sum_{j=1}^{n}\log^+\left|\left|\omega_j^{M_j}\right|\right|_v\right)\\ &= \log {b_v}^{(d_v/d)} + \sum_{j=1}^{n} M_j \log^+|\omega|_v\end{aligned}$$

As before, let $\mathcal{A}_{\mathbb{K}}$ be the set of places of $\mathbb{K}$. From Theorems 1.5.3 (The Product Formula) and 1.6.1 (The Galois Action on Places) we have

$$\begin{aligned}0 &= \sum_{\mathcal{A}_{\mathbb{K}}}\log|\delta|_v\\ &= \sum_{v\mid\infty}\left(\log {a_v}^{(d_v/d)} + \sum_{j=1}^{n} M_j\log^+|\omega_j|_v\right) + \sum_{v\nmid\infty}\left(\log {b_v}^{(d_v/d)} + \sum_{j=1}^{n} M_j\log^+|\omega_j|_v\right)\\ &= \log B + \log A + M\cdot h(\omega) \qquad (2.5.2)\end{aligned}$$

From inequality (1.1.1), equation (1.5.2) and the ordinary triangle inequality we deduce that $B \leq 1$ and $A \leq L$. $\square$

Lemma 2.5.3. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$. Let $p \in \mathbb{N}$ be an odd rational prime that does not ramify in $\mathbb{K}$. Let $\mathcal{A}_p = \{v_1, \ldots, v_t\}$ (where $t \in \mathbb{N}$) be the finite set of places of $\mathbb{K}$ that restrict to the $p-$adic place of $\mathbb{Q}$. For $v_i \in \mathcal{A}_p$, let $\mathrm{Z}_{v_i} = \langle \Phi_{v_i} \rangle \leq \mathrm{G}$ be the stabilizer of v_i. Let $s \in \mathbb{N}$ and $n = [\mathrm{G} : \mathrm{Z}_{\mathrm{G}}(\Phi_{v_i}^s)]$. If*

$$m \in \mathbb{N} \text{ such that } p^{m/n} > 2$$

and

$$\beta \in \mathbb{K}^{\times} - \mathrm{Tor}(\mathbb{K}^{\times})$$

Then

$$h(\beta) \geq \left(\frac{\log p^{m/n} - \log 2}{p^{m-1} \cdot (1 + p^s)} \right) \tag{2.5.3}$$

Proof. From Theorem 1.9.1(i) we can assume, without a loss of generality, that

$$\Phi_{v_1}^s = \cdots = \Phi_{v_{t/n}}^s \tag{2.5.4}$$

Let $\mathcal{R}_\beta$ be the subset of $\{ v_1, \ldots, v_{t/n} \}$ such that $\beta \in \mathcal{O}_{v_i}$ and let $\mathcal{S}_\beta = \{ v_1, \ldots, v_{t/n} \} - \mathcal{R}_\beta$. For $v_i \in \mathcal{R}_\beta$ we have by inclusion (1.9.9) that

$$\Phi_{v_1}^s(\beta) - \beta^{p^s} \in \mathcal{M}_{v_i} \tag{2.5.5}$$

From the Binomial Theorem

$$\left(\Phi_{v_1}^s(\beta) - \beta^{p^s} \right)^p = \sum_{j=0}^{(p-1)/2} \binom{p}{j} \Phi_{v_1}^s(\beta^j) \beta^{p^s \cdot j} \left(\Phi_{v_1}^s(\beta^{p-2j}) - \beta^{p^s(p-2j)} \right) \tag{2.5.6}$$

For each $j \in \{ 1, \ldots, (p-1)/2 \}$ the binomial coefficient $\binom{p}{j}$ is divisible by p and is hence in $\mathcal{M}_{v_i}$. Since

$$\left(\Phi_{v_1}^s(\beta) - \beta^{p^s} \right)^p \in \mathcal{M}_{v_i}^p \tag{2.5.7}$$

and $\mathcal{M}_{v_i}$ is an ideal of $\mathcal{O}_{v_i}$ we have

$$\Phi^s_{v_1}(\beta^p) - \beta^{p^{s+1}} \ \in \ \mathcal{M}^2_{v_i} \tag{2.5.8}$$

By induction we have

$$\Phi^s_{v_1}(\beta^{p^{m-1}}) - \beta^{p^{s+m-1}} \ \in \ \mathcal{M}^m_{v_i} \tag{2.5.9}$$

Moreover, from Lemma 2.2.3 we know that

$$\Phi^s_{v_1}(\beta^{p^{m-1}}) - \beta^{p^{s+m-1}} \ \neq \ 0$$

For each $v_i \ \in \ \{ \ v_1, \ \ldots \ , \ v_{t/n} \ \}$ define b_{v_i} as

$$b_{v_i} \ \equiv \ \frac{\left| \ \Phi^s_{v_1}(\beta^{p^{m-1}}) - \beta^{p^{s+m-1}} \ \right|_{v_i}}{\max\left\{ \ 1, \ \left| \ \Phi^s_{v_1}(\beta^{p^{m-1}}) \ \right|_{v_i} \right\} \cdot \max\left\{ \ 1, \ \left| \ \beta^{p^{s+m-1}} \ \right|_{v_i} \right\}} \tag{2.5.10}$$

From Lemma 2.5.1 and inequality (2.5.9), for $v_i \ \in \ \mathcal{R}_\beta$ we have

$$b_{v_i} \ \leq \ p^{-m/t} \tag{2.5.11}$$

For $v_i \ \in \ \mathcal{S}_\beta$ it follows from the ultrametric inequality, and the fact that $m > 0$, that

$$b_{v_i} = \frac{1}{\left| \ \Phi_{v_1}(\beta^{p^{m-1}}) \ \right|_{v_i}} \ \leq \ p^{-m/t} \tag{2.5.12}$$

it follows that

$$\prod_{i=1}^{t/n} b_{v_i} \ \leq \ p^{-m/n} \tag{2.5.13}$$

It then follows from Lemma 2.5.2 that

$$p^{m-1} \cdot (1 + p^s) \cdot h(\beta) \ \geq \ \log p^{m/n} - \log 2 \quad \square$$

Lemma 2.5.4. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension such that 2 does not ramify in $\mathbb{K}$. Let* $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$. *Let* $\mathcal{A}_2 = \{ v_1, \ldots, v_t \}$ *(where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the $2-$adic place of $\mathbb{Q}$. For $v_i \in \mathcal{A}_2$, let* $\mathrm{Z}_{v_i} = \langle \Phi_{v_i} \rangle \leq G$ *be the stabilizer of v_i. Let $s \in \mathbb{N}$ and let* $n = [\mathrm{G} : \mathrm{Z}_{\mathrm{G}}(\Phi_{v_i}^s)]$.
If $m \in \mathbb{N}$ such that *$m > n$ and $\beta \in \mathbb{K}^{\times} - \mathrm{Tor}(\mathbb{K}^{\times})$ then*

$$h(\beta) \ \geq \ \left(\frac{m-n}{n} \right) \cdot \left(\frac{\log 2}{2^{m-1} \cdot (1 + 2^s)} \right) \tag{2.5.14}$$

Proof. From Theorem 1.9.1.(i) we can assume, without a loss of generality, that

$$\Phi_{v_1}^s \ = \ \cdots \ = \ \Phi_{t/n}^s \tag{2.5.15}$$

Let $\mathcal{R}_\beta$ be the subset of $\{ v_1, \ldots, v_{t/n} \}$ such that $\beta \in \mathcal{O}_{v_i}$ and let $\mathcal{S}_\beta = \{ v_1, \ldots, v_{t/n} \} - \mathcal{R}_\beta$. For $v_i \in \mathcal{R}_\beta$ we have by inclusion (1.9.9) that

$$\Phi_{v_1}^s(\beta) - \beta^{2^s} \ \in \ \mathcal{M}_{v_i} \tag{2.5.16}$$

Since

$$2 \cdot \beta^{2^s} \ \in \ \mathcal{M}_{v_i} \tag{2.5.17}$$

and $\mathcal{M}_{v_i}$ is an ideal it follows from inclusions (2.5.16) and (2.5.17) that

$$\Phi_{v_1}^s(\beta) + \beta^{2^s} \ \in \ \mathcal{M}_{v_i} \tag{2.5.18}$$

from the difference of squares formula it follows from inclusions (2.5.16) and (2.5.18) that

$$\Phi^s_{v_1}(\beta^2) - \beta^{2^{s+1}} \ \in \ \mathcal{M}^2_{v_i} \tag{2.5.19}$$

By induction,

$$\Phi^s_{v_1}(\beta^{2^{m-1}}) - \beta^{2^{s+m-1}} \ \in \ \mathcal{M}^m_{v_i} \tag{2.5.20}$$

Moreover, we know from Lemma 2.2.3 that

$$\Phi^s_{v_1}(\beta^{2^{m-1}}) - \beta^{2^{s+m-1}} \ \neq \ 0$$

For each $v_i \ \in \ \{ \ v_1, \ \ldots \ , \ v_t \ \}$ define b_{v_i} by

$$b_{v_i} \ \equiv \ \frac{\left| \ \Phi_{v_1}(\beta^{2^{m-1}}) - \beta^{2^{s+m-1}} \ \right|_{v_i}}{\max\Big\{ \ 1, \ \Big| \ \Phi_{v_1}(\beta^{2^{m-1}}) \ \Big|_{v_i} \Big\} \cdot \max\Big\{ \ 1, \ \Big| \ \beta^{2^{s+m-1}} \ \Big|_{v_i} \Big\}} \tag{2.5.21}$$

From inclusion (2.5.20) and Lemma 2.5.1 we have that for $v_i \ \in \ \mathcal{R}_\beta$

$$b_{v_i} \ \leq \ 2^{-m/t} \tag{2.5.22}$$

For $v_i \ \in \ \mathcal{S}_\beta$ it follows from inequality (1.1.1) that

$$b_{v_i} = \frac{1}{\left| \ \Phi_{v_1}(\beta^{2^{m-1}}) \ \right|_{v_i}} \leq 2^{-m/t} \tag{2.5.23}$$

Consequently,

$$\prod_{i=1}^{t/n} b_{v_i} \ \leq \ 2^{-m/n} \tag{2.5.24}$$

It then follows from Lemma 2.5.2 that

$$2^{m-1} \cdot (1 + 2^s) \cdot h(\beta) \ \geq \ \left(\frac{m-n}{n} \right) \cdot \log 2 \qquad \square$$

Lemma 2.5.5. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with $\mathrm{G} = \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $p \in \mathbb{N}$ be an odd prime that ramifies in $\mathbb{K}$ with ramification index e. Let v_1 be a place of $\mathbb{K}$ restricting to the $p-$adic place of $\mathbb{Q}$. For $j \in \{0\} \bigcup \mathbb{N}$ let $\mathrm{G}_{v_1,j} \leq \mathrm{G}$ be the $j-$th ramification group of v_1. Let $m \in \{0\} \bigcup \mathbb{N}$ be maximal such that $\mathrm{G}_{v_1,m} \neq \{1\}$. Let $n = [\mathrm{G} : \mathrm{N}_{\mathrm{G}}(\mathrm{G}_{v_1,m})]$. Let $a \in \{0\} \bigcup \mathbb{N}$ be maximal such that $p^{a-1}(m+1)(p-1) \leq e$. For $r \in \{0\} \bigcup \mathbb{N}$ define $\omega_p(r, \mathbb{K}) \in \mathbb{N}$ by*

$$\omega_p(r, \mathbb{K}) = \begin{cases} p^r \cdot (m+1) & \text{if } \ r \leq a \\ p^a \cdot (m+1) + (r-a) \cdot e & \text{if } \ r > a \end{cases}$$

If $s \in \mathbb{N} \bigcup \{0\}$, $\beta \in \mathbb{K}^{\times} - \mathrm{Tor}(\ \mathbb{K}^{\times}\ )$, and $\sigma \in \mathrm{G}_{v_1,m}$ such that

$$\Big(\log p \Big) \cdot \Big(\ \omega_p(s, \mathbb{K}) \ \Big) \ > \ \Big(\log 2 \Big) \cdot \Big(\ e \cdot n \ \Big)$$

and

$$0 \ \neq \ \beta^{p^s} - \sigma(\beta^{p^s})$$

then

$$h(\beta) \ \geq \ \left(\frac{\omega_p(s, \mathbb{K})}{e \cdot n} \right) \cdot \left(\ \frac{\log p - \log 2}{2 \cdot p^s} \ \right) \tag{2.5.25}$$

Proof. Let $\mathcal{A}_p = \{\ v_1, \ \ldots, \ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the $p-$adic place on $\mathbb{Q}$. For $v_j \in \mathcal{A}_p$ and $k \in \mathbb{N} \bigcup \{\ 0\ \}$ let $\mathrm{G}_{v_j,k}$ be the

$k-th$ ramification group of v_j. From Theorem 1.9.1(i) for each $v_j \in \mathcal{A}_p$ there exists $g_{1j} \in \mathrm{G}$ such that

$$\mathrm{G}_{v_j,m} = g_{1j} \ \mathrm{G}_{v_1,m} \ g_{1j}^{-1} \tag{2.5.26}$$

We may thus suppose, without a loss of generality, that

$$\mathrm{G}_{v_1,m} = \cdots = \mathrm{G}_{v_{t/n},m} \tag{2.5.27}$$

Let $\mathcal{R}_\beta$ be the subset of $\{ v_1, \ldots, v_{t/n} \}$ such that $\beta \in \mathcal{O}_{v_i}$ and let $\mathcal{S}_\beta = \{ v_1, \ldots, v_{t/n} \} - \mathcal{R}_\beta$. From equation (1.9.7) we have for all $v_j \in \mathcal{R}_\beta$

$$\beta - \sigma(\beta) \in \mathcal{M}_{v_j}^{m+1} \tag{2.5.28}$$

and consequently

$$\left(\beta - \sigma(\beta) \right)^p \in \mathcal{M}_{v_j}^{(m+1)\cdot p} \tag{2.5.29}$$

From the Binomial Theorem

$$\left(\beta - \sigma(\beta) \right)^p = \sum_{i=0}^{(p-1)/2} \binom{p}{i} \big(\beta \cdot \sigma(\beta)\big)^i \cdot \left(\beta^{p-2i} - \sigma(\beta)^{p-2i} \right) \tag{2.5.30}$$

For $j \in \{ 1, \ldots, (p-1)/2 \}$ the binomial coefficient $\left(\begin{array}{c} p \\ j \end{array} \right)$ is divisible by p. It consequently follows that

$$\beta^p - \sigma(\beta^p) \in \mathcal{M}_{v_j}^{\omega_p(1,\mathbb{K})} \tag{2.5.31}$$

By induction, for all $s \in \mathbb{N}$

$$\beta^{p^s} - \sigma(\beta^{p^s}) \in \mathcal{M}_{v_j}^{\omega_p(s,\mathbb{K})} \tag{2.5.32}$$

Suppose now that $v_j \in \mathcal{S}_\beta$. Then $1/\beta \in \mathcal{O}_{v_j}$ and we can deduce that

$$\frac{\beta^{p^s} - \sigma(\beta^{p^s})}{\beta^{p^s} \cdot \sigma(\beta^{p^s})} \in \mathcal{M}_{v_j}^{\omega_p(s,\mathbb{K})} \tag{2.5.33}$$

For each $v_j \in \mathcal{A}_p$ define b_{v_j} by

$$b_{v_j} \equiv \frac{\left| \beta^{p^s} - \sigma(\beta^{p^s}) \right|_{v_j}}{\max\left\{ 1, \left| \beta^{p^s} \right|_{v_j} \right\} \cdot \max\left\{ 1, \left| \sigma(\beta^{p^s}) \right|_{v_j} \right\}} \tag{2.5.34}$$

For $v_j \in \mathcal{R}_\beta$ it follows from Lemma 2.5.1 and inclusion (2.5.32) that

$$b_{v_j} \leq p^{\frac{-\omega_p(s,\mathbb{K})}{e \cdot t}} \tag{2.5.35}$$

For $v_j \in \mathcal{S}_\beta$ it follows from Lemma 2.5.1 and inclusion (2.5.33) that

$$b_{v_j} \leq p^{\frac{-\omega_p(s,\mathbb{K})}{e \cdot t}} \tag{2.5.36}$$

Consequently,

$$\prod_{i=1}^{t} b_{v_i} \leq p^{\frac{-\omega_p(s,\mathbb{K})}{e \cdot n}} \tag{2.5.37}$$

It follows from inequality (2.5.37) and Lemma 2.5.2 that

$$2 \cdot p^s \cdot h(\beta) \geq \left(\frac{\omega_p(s,\mathbb{K})}{e \cdot n} \right) \cdot \log p - \log 2 \quad \square$$

Lemma 2.5.6. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$. Suppose that 2 ramifies in $\mathbb{K}$ with ramification index e. Let v_1 be a place of $\mathbb{K}$ re-*

stricting to the $2-$*adic place of* $\mathbb{Q}$*. For* $j \in \{0\} \bigcup \mathbb{N}$*, let* $\mathrm{G}_{v_1,j} \leq \mathrm{G}$ *be the* $j-$*th ramification group of* v_1*. Let* $m \in \mathbb{N} \bigcup \{0\}$ *be maximal such that* $\mathrm{G}_{v_1,m} \neq \{1\}$*. Let* $n = [\mathrm{G} : \mathrm{N}_{\mathrm{G}}(\mathrm{G}_{v_1,m})]$ *and* $a \in \{0\} \bigcup \mathbb{N}$ *maximal such that* $2^{a-1}(m+1) \leq e$*. For* $r \in \{0\} \bigcup \mathbb{N}$ *define* $\omega_2(r, \mathbb{K})$ *by*

$$\omega_2(r, \mathbb{K}) = \begin{cases} 2^r \cdot (m+1) & \text{if } r \leq a \\ 2^a \cdot (m+1) + (r-a) \cdot e & \text{if } r > a \end{cases}$$

If $s \in \mathbb{N} \bigcup \{ 0 \}$, $\beta \in \mathbb{K}^{\times} - \mathrm{Tor}(\mathbb{K}^{\times})$ *and* $\sigma \in \mathrm{G}_{v_1,m}$ *such that*

$$\omega_2(s, \mathbb{K}) > \left(e \cdot n \right)$$

and

$$0 \neq \beta^{2^s} - \sigma(\beta^{2^s})$$

then

$$h(\beta) \geq \left(\frac{\omega_2(s, \mathbb{K}) - e \cdot n}{e \cdot n} \right) \cdot \left(\frac{\log 2}{2^{s+1}} \right) \tag{2.5.38}$$

Proof. Let $\mathcal{A}_2 = \{ v_1, \ldots, v_t \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the 2−adic place of $\mathbb{Q}$. For $v_j \in \mathcal{A}_2$ and $k \in \mathbb{N} \bigcup \{ 0 \}$ let $\mathrm{G}_{v_j,k}$ be the $k-$th ramification group of v_j. By Theorem 1.9.1(i) for each $v_j \in \mathcal{A}_2$ there exists $g_{1j} \in \mathrm{G}$ such that

$$\mathrm{G}_{v_j,m} = g_{1j} \ \mathrm{G}_{v_1,m} \ g_{1j}^{-1} \tag{2.5.39}$$

We can thus assume, without a loss of generality, that

$$\mathrm{G}_{v_1,m} = \cdots = \mathrm{G}_{v_{t/n},m} \tag{2.5.40}$$

Let $\mathcal{R}_\beta$ be the subset of $\{ v_1, \ldots, v_{t/n} \}$ such that $\beta \in \mathcal{O}_{v_i}$ and let $\mathcal{S}_\beta = \{ v_1, \ldots, v_{t/n} \} - \mathcal{R}_\beta$. From equation (1.9.7) we have for all $v_j \in \mathcal{R}_\beta$ that

$$\beta - \sigma(\beta) \in \mathcal{M}_{v_j}^{m+1} \tag{2.5.41}$$

Since $2 \cdot \sigma(\beta) \in \mathcal{M}_{v_j}$ and $\mathcal{M}_{v_j}$ is an ideal we have

$$\beta + \sigma(\beta) \in \mathcal{M}_{v_j}^{\min\{ m+1, e \}} \tag{2.5.42}$$

From the difference of squares formula and inclusions (2.5.41) and (2.5.42)

$$\beta^2 - \sigma(\beta^2) \in \mathcal{M}_{v_j}^{\omega_2(1,\mathbb{K})} \tag{2.5.43}$$

by induction

$$\beta^{2^s} - \sigma(\beta^{2^s}) \in \mathcal{M}_{v_j}^{\omega_2(s,\mathbb{K})} \tag{2.5.44}$$

For $v_j \in \mathcal{S}_\beta$, $1/\beta \in \mathcal{O}_{v_j}$ and it follows similarly that

$$\frac{\beta^{2^s} - \sigma(\beta^{2^s})}{\beta^{2^s} \cdot \sigma(\beta^{2^s})} \in \mathcal{M}_{v_j}^{\omega_2(s,\mathbb{K})} \tag{2.5.45}$$

For $v_j \in \{ v_1, \ldots, v_{t/n} \}$ define b_{v_j} by

$$b_{v_j} \equiv \frac{\left| \beta^{2^s} - \sigma(\beta^{2^s}) \right|_{v_j}}{\max\left\{ 1, \left| \beta^{2^s} \right|_{v_j} \right\} \cdot \max\left\{ 1, \left| \sigma(\beta^{2^s}) \right|_{v_j} \right\}} \tag{2.5.46}$$

For $v_j \in \mathcal{R}_\beta$ it follows from Lemma 2.5.1 and inclusion (2.5.43) that

$$b_{v_j} \leq 2^{-\omega_2(s,\mathbb{K})/et} \tag{2.5.47}$$

For $v_j \in \mathcal{S}_\beta$ it follows from Lemma 2.5.1 and inclusion (2.5.45) that

$$b_{v_j} \leq 2^{-\omega_2(s,\mathbb{K})/et} \tag{2.5.48}$$

Consequently,

$$\prod_{i=1}^{t/n} b_{v_i} \leq 2^{-\omega_2(s,\mathbb{K})/en} \tag{2.5.49}$$

It follows from inequality (2.5.49) and Lemma 2.5.2 that

$$2^{s+1} \cdot h(\beta) \geq \left(\frac{\omega_2(s,\mathbb{K}) - e \cdot n}{e \cdot n} \right) \cdot \log 2 \quad \square$$

Lemma 2.5.7. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $p \in \mathbb{N}$ be a rational prime that ramifies in $\mathbb{K}$ with ramification index e. Let v_1 be a place of $\mathbb{K}$ restricting to the $p-$adic place of $\mathbb{Q}$. Let $\Phi_{v_1} \in \mathrm{G}$ act as a generator of $\mathrm{Aut}(\ \mathbb{F}_{v_1}\ /\ \mathbb{F}_p\ )$. Let $s \in \mathbb{N}$ and $n = [\mathrm{G} : \mathrm{Z}_{\mathrm{G}}(\Phi_{v_1}^s)]$. Let $a \in \mathbb{N} \bigcup \{0\}$ be maximal such that $p^{a-1}(p-1) \leq e$. For $r \in \mathbb{N} \bigcup \{0\}$ define $\omega_p(r,\mathbb{K})$ by*

$$\omega_p(r,\mathbb{K}) = \begin{cases} p^r & \text{if } r \leq a \\ p^a + (r-a) \cdot e & \text{if } r \geq a \end{cases}$$

If

$$\Big(\ \omega_p(r,\mathbb{K})\ \Big) \cdot \Big(\ \log p\ \Big) > \Big(\ \log 2\ \Big) \cdot \Big(\ e \cdot n\ \Big)$$

and

$$\beta \in \mathbb{K}^\times - \mathrm{Tor}(\ \mathbb{K}^\times\ )$$

then

$$h(\beta) \geq \left(\frac{\omega_p(r, \mathbb{K})}{e \cdot n} \right) \cdot \left(\frac{\log p - \log 2}{p^r \cdot (1 + p^s)} \right) \tag{2.5.50}$$

Proof. Let $\mathcal{A}_p = \{ v_1, \ldots, v_t \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the $p-$adic place of $\mathbb{Q}$ and let $\Phi_{v_i} \in \mathrm{G}$ act as a generator of $\mathrm{Aut}(\mathbb{F}_{v_i} / \mathbb{F}_p)$. By Theorem 1.9.1(i), for $v_j \in \mathcal{A}_p$ there exists $g_{1j} \in \mathrm{G}$ such that

$$\Phi_{v_j}^s = g_{1j} \ \Phi_{v_1}^s \ g_{1j}^{-1} \tag{2.5.51}$$

We may thus assume, without a loss of generality, that

$$\Phi_{v_1}^s = \cdots = \Phi_{v_{t/n}}^s \tag{2.5.52}$$

Let $\mathcal{R}_\beta$ be the subset of $\{ v_1, \ldots, v_{t/n} \}$ such that $\beta \in \mathcal{O}_{v_i}$ and let $\mathcal{S}_\beta = \{ v_1, \ldots, v_{t/n} \} - \mathcal{R}_\beta$. For $v_j \in \mathcal{R}_\beta$ it follows from inclusion (1.9.9) that

$$\Phi_{v_1}^s(\beta) - \beta^{p^s} \in \mathcal{M}_{v_j} \tag{2.5.53}$$

From the Binomial Theorem

$$\left(\Phi_{v_1}^s(\beta) - \beta^{p^s} \right)^p = \sum_{j=0}^{(p-1)/2} \binom{p}{j} \Phi_{v_1}^s(\beta^j) \cdot \beta^{p^s \cdot j} \left(\Phi_{v_1}^s(\beta^{p-2j}) - \beta^{(p^s)(p-2j)} \right) \tag{2.5.54}$$

For each $j \in \{ 1, \ldots, (p-1)/2 \}$ the bimiomial coefficient $\binom{p}{j}$ is divisible by $p \in \mathcal{M}_{v_j}^e$. Since $\mathcal{M}_{v_j}$ is a ring and

$$\left(\Phi_{v_1}^s(\beta) - \beta^{p^s} \right)^p \in \mathcal{M}_{v_1}^p \tag{2.5.55}$$

we have that

$$\Phi^s_{v_1}(\beta^p) - \beta^{p^{s+1}} \ \in \ \mathcal{M}_{v_1}^{\omega_p(1,\mathbb{K})} \tag{2.5.56}$$

and by induction

$$\Phi^s_{v_1}(\beta^{p^r}) - \beta^{p^{s+r}} \ \in \ \mathcal{M}_{v_1}^{\omega_p(r,\mathbb{K})} \tag{2.5.57}$$

For $v_j \ \in \ \mathcal{S}_\beta, \ 1/\beta \ \in \ \mathcal{O}_{v_j}$ and it follows from the same sequence of steps that led to inclusion (2.5.57) that

$$\frac{\Phi^s_{v_1}(\beta^{p^r}) - \beta^{p^{r+s}}}{\Phi^s_{v_1}(\beta^{p^r}) \cdot \beta^{p^{r+s}}} \ \in \ \mathcal{M}_{v_1}^{\omega_p(r,\mathbb{K})} \tag{2.5.58}$$

For each $v_i \ \in \ \{ \ v_1, \ \ldots \ , \ v_{t/n} \ \}$ define b_{v_i} by

$$b_{v_i} \ \equiv \ \frac{\left| \ \Phi^s_{v_1}(\beta^{p^r}) - \beta^{p^{r+s}} \ \right|_{v_i}}{\max\left\{ \ 1, \ \left| \ \Phi^s_{v_1}(\beta^{p^r}) \ \right|_{v_i} \right\} \cdot \max\left\{ \ 1, \ \left| \ \beta^{p^{r+s}} \ \right|_{v_i} \right\}} \tag{2.5.59}$$

It follows from Lemma 2.5.1 and inclusion (2.5.57) that for $v_i \ \in \ \mathcal{R}_\beta$

$$b_{v_i} \ \leq \ p^{-\omega_p(r,\mathbb{K})/et} \tag{2.5.60}$$

It follows from inequality (1.1.1) and inclusion (2.5.58) that for $v_i \ \in \ \mathcal{S}_\beta$

$$b_{v_i} \ \leq \ p^{-\omega_p(r,\mathbb{K})/et} \tag{2.5.61}$$

Consequently

$$\prod_{i=1}^{t/n} b_{v_i} \ \leq \ p^{-\omega_p(r,\mathbb{K})/en} \tag{2.5.62}$$

It follows from Lemma 2.5.2 that

$$p^r \cdot (1 + p^s) \cdot h(\beta) \geq \left(\frac{\omega_p(r, \mathbb{K})}{e \cdot n} \right) \cdot \log p - \log 2 \qquad \square$$

Lemma 2.5.8. *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension with* $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. *Suppose that* 2 *ramifies in* $\mathbb{K}$ *with ramification index* e *and let* v_1 *be a place of* $\mathbb{K}$ *restricting to the* $2-$*adic place of* $\mathbb{Q}$. *Let* $\Phi_{v_1} \in \mathrm{G}$ *act as a generator of* $\mathrm{Aut}(\ \mathbb{F}_{v_1}\ /\ \mathbb{F}_2\ )$. *Let* $s \in \mathbb{N}$ *and* $n = [\mathrm{G} : \mathrm{Z}_{\mathrm{G}}(\Phi_{v_1}^s)]$. *Let* $a \in \mathbb{N} \bigcup \{0\}$ *be maximal such that* $2^{a-1} \leq e$. *For* $r \in \mathbb{N} \bigcup \{0\}$ *define* $\omega_2(r, \mathbb{K})$ *by*

$$\omega_2(r, \mathbb{K}) = \begin{cases} 2^r & \text{if } \ r \leq a \\ 2^a + (r - a) \cdot e & \text{if } \ r > a \end{cases}$$

If

$$\omega_2(r, \mathbb{K}) > \left(\ e \cdot n\ \right)$$

and

$$\beta \in \mathbb{K}^\times \ - \ \mathrm{Tor}(\ \mathbb{K}^\times\ )$$

then

$$h(\beta) \ \geq \ \left(\frac{\omega_2(r, \mathbb{K}) - en}{e \cdot n} \right) \cdot \left(\ \frac{\log 2}{2^r \cdot (1 + 2^s)}\ \right) \tag{2.5.63}$$

Proof. Let $\mathcal{A}_2 \ = \ \{\ v_1,\ \ldots\ ,\ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the $2-$adic place of $\mathbb{Q}$. For $v_i \in \mathcal{A}_2$ let $\Phi_{v_i} \in \mathrm{G}$ act as a generator of $\mathrm{Aut}(\ \mathbb{F}_{v_i}\ /\ \mathbb{F}_2\ )$. By Theorem 1.9.1(i) for $v_j \in \mathcal{A}_2$ there exists $g_{1j} \in \mathrm{G}$ such that

$$\Phi_{v_j}^s \ = \ g_{1j} \ \ \Phi_{v_1}^s \ \ g_{1j}^{-1} \tag{2.5.64}$$

We can thus suppose, without a loss of generality, that

$$\Phi_{v_1}^s \;=\; \cdots \;=\; \Phi_{v_{t/n}}^s \tag{2.5.65}$$

Let $\mathcal{R}_\beta$ be the subset of $\{\ v_1,\ \ldots,\ v_{t/n}\ \}$ such that $\beta \;\in\; \mathcal{O}_{v_i}$ and let $\mathcal{S}_\beta \;=\; \{\ v_1,\ \ldots,\ v_{t/n}\ \} \;-\; \mathcal{R}_\beta$. For $v_i \;\in\; \mathcal{R}_\beta$ it follows from inclusion (1.9.9) that

$$\Phi_{v_1}^s(\beta) - \beta^{2^s} \;\in\; \mathcal{M}_{v_i} \tag{2.5.66}$$

Since $\mathcal{M}_{v_i}$ is an ideal, $2 \cdot \beta^{p^s} \;\in\; \mathcal{M}_{v_i}$ and

$$\Phi_{v_1}^s(\beta) + \beta^{2^s} \;\in\; \mathcal{M}_{v_i} \tag{2.5.67}$$

From the difference of squares formula and inclusions (2.5.66) and (2.5.67)

$$\Phi_{v_1}^s(\beta^2) - \beta^{2^{s+1}} \;\in\; \mathcal{M}_{v_i}^{\omega_2(1,\mathbb{K})} \tag{2.5.68}$$

and by induction

$$\Phi_{v_1}^s(\beta^{2^r}) - \beta^{2^{s+r}} \;\in\; \mathcal{M}_{v_i}^{\omega_2(r,\mathbb{K})} \tag{2.5.69}$$

For $v_j \;\in\; \mathcal{S}_\beta,\quad 1/\beta \;\in\; \mathcal{O}_{v_j}$ and it follows from the same steps that established inclusion (2.5.69) that

$$\frac{\Phi_{v_1}^s(\beta^{2^r}) - \beta^{2^{s+r}}}{\Phi_{v_1}^s(\beta^{2^r}) \cdot \beta^{2^{s+r}}} \;\in\; \mathcal{M}_{v_i}^{\omega_2(r,\mathbb{K})} \tag{2.5.70}$$

For each $v_j \;\in\; \{\ v_1,\ \ldots,\ v_{t/n}\ \}$ define b_{v_j} by

$$b_{v_j} \;\equiv\; \frac{\left|\ \Phi_{v_1}^s(\beta^{2^r}) - \beta^{2^{r+s}}\ \right|_{v_i}}{\max\left\{\ 1,\ \left|\ \Phi_{v_1}^s(\beta^{2^r})\ \right|_{v_i}\right\} \cdot \max\left\{\ 1,\ \left|\ \beta^{2^{r+s}}\ \right|_{v_i}\right\}} \tag{2.5.71}$$

It follows from Lemma 2.5.1 and inclusion (2.5.69) that for $v_j \in \mathcal{R}_\beta$

$$b_{v_j} \leq 2^{-\omega_2(r,\mathbb{K})/et} \tag{2.5.72}$$

It follows from inequality (1.1.1) and inclusion (2.5.70) that for $v_i \in \mathcal{S}_\beta$

$$b_{v_i} \leq 2^{-\omega_2(r,\mathbb{K})/et} \tag{2.5.73}$$

Consequently

$$\prod_{i=1}^{t/n} b_{v_i} \leq 2^{-\omega_2(r,\mathbb{K})/en} \tag{2.5.74}$$

It follows from Lemma 2.5.2 that

$$2^r \cdot (1 + 2^s) \cdot h(\beta) \geq \left(\frac{\omega_2(r,\mathbb{K}) - en}{e \cdot n} \right) \cdot \log 2 \quad \square$$

2.6 An Example

The following is a theorem of Shafarevich [Sha54].

Theorem 2.6.1. (Shafarevich) *Let* G *be a finite solvable group. Then there exists a finite Galois extension* $\mathbb{K}/\mathbb{Q}$ *such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx \mathrm{G}$.

For $n \in \mathbb{N}$ let $\mathbb{E}_{2^n}$ be the elementary abelian group of order 2^n. Then, by Proposi-

tion 17, Section 4.4 of [Dum99],

$$\mathrm{Aut}(\mathbb{E}_{2^n}) \approx \mathrm{GL}_n(\mathbb{F}_2) \tag{2.6.1}$$

we can consequently deduce that there exist groups of the form

$$\mathbb{E}_{2^n} \rtimes_\rho \mathbb{E}_{2^m} \tag{2.6.2}$$

where $ker\rho = \{1\}$ and $\mathbb{E}_{2^m} \leq \mathrm{GL}_n(\mathbb{F}_2)$. From Theorem 2.6.1 there exists an algebraic number field $\mathbb{K}$ such that $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \approx \mathbb{E}_{2^n} \rtimes_\rho \mathbb{E}_{2^m}$. We can use non-archimedean estimates to prove the following result that is similar in its hypothesis and conclusions to Theorem 2.3.2.

Corollary 2.6.2. (Garza) *Let* $m, n \in \mathbb{N}$. *Let* $\mathbb{K}/\mathbb{Q}$ *be a Galois extension such that* $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \approx \mathrm{H} \rtimes_\phi \mathrm{K}$ *where* $\mathrm{H} \approx \mathbb{E}_{2^n}$ and $\mathrm{K} \approx \mathbb{E}_{2^m}$. *Let* $\beta \in \mathbb{K}^\times - \mathrm{Tor}(\mathbb{K}^\times)$. *Then*

$$h(\beta) \geq \left(\frac{1}{82 \cdot 27} \right) \cdot \log\left(\frac{3}{2} \right)$$

Proof. Let $\mathcal{A}_3 = \{ v_1, \ldots, v_t \}$ (where $t \in \mathbb{N}$) be the set places of $\mathbb{K}$ that restrict to the $3-adic$ place of $\mathbb{Q}$. Let e be their common ramification index and f their common residue class degree. It follows from elementary group theory that the commutator G' of G is a subgroup of H. Given $g \in \mathrm{G}$ it follows from the definition of semidirect products that there exists $h_g \in \mathrm{H}$ and $k_g \in \mathrm{K}$ such that $g = h_g k_g$. It then follows that $g^2 = [h_g, k_g] \in \mathrm{G}'$ so that $|g| \leq 4$. Consequently, $f \leq 4$ and from Theorem 1.9.1 e divides $3^4 - 1 = 80$ so that $e \leq 16$. If $e = 1$ it follows from Lemma 2.5.3 that $82 \cdot h(\beta) \geq \log(3/2)$. If $e > 1$ it follows from Lemma 2.5.7 that

$82 \cdot 27 \cdot h(\beta) \geq \log(3/2)$. $\square$

The following Lemma can be found as Proposition 21 in Section 14.4 of [Dum99].

Lemma 2.6.3. (Composition of Galois Extensions) *Let* $\mathbb{K}$ *and* $\mathbb{F}$ *be finite Galois extensions of* $\mathbb{Q}$ *with Galois groups* $\mathrm{G}_{\mathbb{K}}$ and $\mathrm{G}_{\mathbb{F}}$ *respectively. Then the composite field* $\mathbb{F}\mathbb{K}$ *is Galois over* $\mathbb{Q}$ *with Galois group isomorphic to the subgroup*

$$\mathrm{H} \;=\; \left\{ \; (\sigma, \tau) \;:\; \sigma|_{\mathbb{F} \bigcap \mathbb{K}} = \tau|_{\mathbb{F} \bigcap \mathbb{K}} \; \right\}$$

of the direct product $\mathrm{G}_{\mathbb{K}} \times \mathrm{G}_{\mathbb{F}}$ *consisting of elements whose restrictions to the intersection* $\mathbb{K} \bigcap \mathbb{F}$ *are equal.*

Corollary 2.6.4. (Garza) *Let* $\mathbb{E}$ *be the composite of all Galois extensions of* $\mathbb{Q}$ *whose Galois groups are isomorphic to* $\mathrm{B} \rtimes_{\phi} \mathrm{A}$ *where* A *and* B *are elementary abelian* $2-$*groups. Let* $\alpha \in \mathbb{E}^{\times} - \mathrm{Tor}(\, \mathbb{E}^{\times} \,)$. *Then*

$$h(\beta) \;\geq\; \left(\; \frac{1}{82 \cdot 27} \; \right) \cdot \log\left(\; \frac{3}{2} \; \right)$$

Proof. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$. The proof follows by using Lemma 2.6.3 to understand $\mathrm{Aut}(\, \mathbb{K}/\mathbb{Q} \,)$ and by repeating the same steps used in the proof of Corollary 2.6.2. $\square$.

Chapter 3

The Mahler Measure

3.1 Definition

In this section, $||\cdot||_\infty$ will denote the ordinary archimedean absolute value on $\mathbb{C}$. In a 1961 paper [Mah61] K. Mahler defined the *measure* of a polynomial $f(x) \in \mathbb{Z}[x] - \{ 0 \}$ as

$$\log \mathrm{M}(f) \;=\; \int_0^1 \log \Big|\Big| f(e^{2\pi i\theta}) \Big|\Big|_\infty d\theta \tag{3.1.1}$$

In a previous paper [Mah60] Mahler used *Jensen's Formula* from complex analysis to establish the following.

Lemma 3.1.1. (Mahler) *Let $d \in \mathbb{N}$ and $a_0, \ \ldots \ , \ a_d \ \in \ \mathbb{Z}$ such that $a_d \neq 0$ and $a_0 \neq 0$. Let $f(x) \ = \ a_0 x^d + \cdots + a_d = a_0 \cdot \prod_{i=1}^{d} (x - \alpha_i) \ \in \ \mathbb{Z}[x]$. Then*

$$\mathrm{M}(f) \;=\; \Big|\Big| \ a_0 \ \Big|\Big|_\infty \cdot \prod_{i=1}^{d} \max\Big\{ \ 1, \ ||\alpha_i||_\infty \ \Big\} \tag{3.1.2}$$

Let $\mathbb{K}/\mathbb{Q}$ be a finite extension, $p \in \mathbb{N}$ a rational prime, and v a place of $\mathbb{K}$ restricting to the $p-$adic place of $\mathbb{Q}$. Let $\mathbb{K}_v$ be the completion of $\mathbb{K}$ with respect to v. Let $\overline{\mathbb{K}_v}$ be an algebraic closure of $\mathbb{K}_v$. We recall from elementary algebra that the algebraic closures of $\mathbb{K}_v$ are unique up to isomorphism. It can be shown that $\overline{\mathbb{K}_v}$ is not complete (see Theorem 12 of Chapter III of [Kob77]). Let Ω_v be the completion of $\overline{\mathbb{K}_v}$ with respect to the unique extension of $|\cdot|_v$ to $\overline{\mathbb{K}_v}$. It is a theorem that Ω_v is algebraically closed (Theorem 13 of Chapter III of [Kob77]).

Lemma 3.1.2. *Let α be a nonzero algebraic number, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, and let $m_{\alpha,\mathbb{Z}}$ be the minimal polynomial of α over $\mathbb{Z}$. Then*

$$\log \mathrm{M}(m_{\alpha,\mathbb{Z}}) \;=\; d \cdot h(\alpha) \tag{3.1.3}$$

Proof. Let α be a nonzero algebraic number of degree d over $\mathbb{Q}$, let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$, and let

$$m_{\alpha,\mathbb{Q}}(x) \;=\; x^d + a_1 x^{d-1} + \cdots + a_{d-1}x + a_d \tag{3.1.4}$$

be the minimal polynomial of α over $\mathbb{Q}$. Let $\alpha = \alpha_1, \ \ldots \ , \ \alpha_d$ be the set of Galois conjugates of α. Then

$$m_{\alpha,\mathbb{Q}}(x) \;=\; \prod_{i=1}^{d}(x - \alpha_i) \tag{3.1.5}$$

Let v be a place of $\mathbb{K}$ and define

$$\mu_v(\alpha) \;=\; \prod_{i=1}^{d} \max\Big\{\; 1,\; |\alpha_i|_v \;\Big\} \tag{3.1.6}$$

Now restrict v to be non-archimedean and define

$$H_v(\alpha) \;=\; \max\Big\{\; 1,\; |a_1|_v,\; \ldots\,,\; |a_d|_v \;\Big\} \tag{3.1.7}$$

and

$$\nu_v(\alpha) \;=\; \sup\Big\{\; \Big|m_{\alpha,\mathbb{Q}}(z)\Big|_v \;:\; z \;\in\; \Omega_v \text{ and } |z|_v \leq 1 \;\Big\} \tag{3.1.8}$$

For $1 \leq i \leq d$ let e_i be the $i-$th elementary symmetric polynomial in $\alpha_1,\; \ldots\,,\; \alpha_d$ and recall from elementary algebra that $a_i \;=\; (-1)^{d-i} \cdot e_i$. From inequality (1.1.1) it follows that

$$|a_i|_v \;\leq\; \max\Big\{\; \Big|\alpha_{n_1} \cdots \alpha_{n_i}\Big|_v \;:\; n_1 < \cdots < n_i \;\Big\} \tag{3.1.9}$$

and hence that

$$|a_i|_v \;\leq\; \prod_{i=1}^{d} \max\Big\{\; 1,\; |\alpha_i|_v \;\Big\} \;=\; \mu_v(\alpha) \tag{3.1.10}$$

and consequently that

$$H_v(\alpha) \;\leq\; \mu_v(\alpha) \tag{3.1.11}$$

Define

$$\mathcal{R}_v \;=\; \Big\{\; z \;\in\; \Omega_v : |z|_v \;\leq\; 1 \;\Big\} \tag{3.1.12}$$

and

$$\mathcal{M}_v \;=\; \Big\{\; z \;\in\; \Omega_v : |z|_v \;<\; 1 \;\Big\} \tag{3.1.13}$$

$\mathcal{R}_v$ is an integral domain with unique maximal ideal $\mathcal{M}_v$. The residue class field $\mathcal{R}_v$ / $\mathcal{M}_v$ is infinite [Val07]. It consequently follows, using equation (1.1.2), the case of equality in the strong triangle inequality, that there exists $\zeta \in \mathcal{R}_v$ such that $|\zeta|_v = 1$ and for all $1 \leq i \leq d$

$$\Big| \zeta - \alpha_i \Big|_v = \max\Big\{ 1, |\alpha_i|_v \Big\} \tag{3.1.14}$$

It thus follows that

$$\mu_v(\alpha) = \Big| m_{\alpha,\mathbb{Q}}(\zeta) \Big|_v \leq \nu_v(\alpha) \tag{3.1.15}$$

For any $z \in \mathcal{R}_v$ we have by inequality (1.1.1) that

$$\begin{aligned} \Big| m_{\alpha,\mathbb{Q}}(z) \Big|_v &= \Big| z^d + a_1 z^{d-1} + \cdots + a_d \Big|_v \\ &\leq \max\Big\{ 1, |a_1|_v , \ldots , |a_d|_v \Big\} \\ &= H_v(\alpha) \end{aligned}$$

We have thus established the inequalities

$$H_v(\alpha) \leq \mu_v(\alpha) \leq \nu_v(\alpha) \leq H_v(\alpha) \tag{3.1.16}$$

From which it follows that

$$H_v(\alpha) = \mu_v(\alpha) = \nu_v(\alpha) \tag{3.1.17}$$

Let $\mathcal{A}_{\mathbb{Q}(\alpha)}$ be the set of places of $\mathbb{Q}(\alpha)$ and define

$$\mu(\alpha) \;=\; \prod_{\mathcal{A}_{\mathbb{Q}(\alpha)}} \mu_v(\alpha) \tag{3.1.18}$$

It follows from Theorem 1.6.1 that

$$\log \mu(\alpha) \;=\; [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha) \tag{3.1.19}$$

Let $p \in \mathbb{N}$ be a rational prime and let $\mathcal{A}_p = \{ v_1, \ldots, v_t \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the $p-$adic place of $\mathbb{Q}$. From $a_i = (-1)^{d-i} \cdot e_i$ and the Galois action on places, it follows that for v_i and $v_j \in \mathcal{A}_p$

$$H_{v_i}(\alpha) \;=\; H_{v_j}(\alpha) \tag{3.1.20}$$

It follows from equations (2.1.1) and (1.5.0) that

$$\prod_{v \nmid \infty} H_v(\alpha) \;\in\; \mathbb{Z} \tag{3.1.21}$$

We thus define

$$\mathcal{C}_\alpha \;\equiv\; \prod_{v \nmid \infty} H_v \;\in\; \mathbb{Z} \tag{3.1.22}$$

and note that

$$m_{\alpha,\mathbb{Z}}(x) \;=\; \mathcal{C}_\alpha \cdot m_{\alpha,\mathbb{Q}}(x) \tag{3.1.23}$$

By considering equations (3.1.2), (3.1.19), and (3.1.23) the proof of Lemma 3.1.2 is complete. □

It follows from Lemma 3.1.2 that, for a nonzero algebraic number α we may define

$$\mathrm{M}(\alpha) \;=\; \mathrm{M}(m_{\alpha,\mathbb{Z}}) \;=\; e^{d\cdot h(\alpha)} \tag{3.1.24}$$

3.2 Lehmer's Problem

It follows from equation (3.1.1) that for $f, g \in \mathbb{Z}[x]$

$$\mathrm{M}(f \cdot g) \;=\; \mathrm{M}(f) \cdot \mathrm{M}(g) \tag{3.2.1}$$

Using equation (3.2.1) we can restate Theorem 2.2.1 as follows

Lemma 3.2.1. (Kronecker) *Let* $f \in \mathbb{Z}[x]$. *Then* $\mathrm{M}(f) = 1$ *if and only if* $\pm f$ *is a product of a power of* x *and cyclotomic polynomials.*

Proof. By equation (3.2.1) we can suppose that f is irreducible. By Theorem 2.2.1 and Lemma 3.1.2. it follows that f is x or is a cyclotomic polynomial. □

In 1933 D. Lehmer [Leh33] asked the following question

> The following problem arises immediatley. If ϵ is a positive quantity, to find a polynomial of the form
>
> $$f(x) = x^r + a_1 x^{r-1} + \cdots + a_r$$
>
> where the a's are integers, such that the absolute value of the product

of those roots of f which lie outside the unit circle, lies between 1 and $1+\epsilon$.

This problem is known as **Lehmer's Problem.** Lehmer analyzed polynomials of low degree and identified

$$l(x) \;=\; x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1$$

as his lowest known Mahler measure (other than 1). $\mathrm{M}(l) \;\approx\; 1.1762808$ remains the lowest known Mahler measure (other than 1) to this day.

3.3 Reciprocal Polynomials

A polynomial $f \;\in\; \mathbb{Z}[x] - \{\ 0\ \}$ is said to be *reciprocal* if

$$f(x) \;=\; \left(\ x^{deg\ f}\ \right) \cdot f\left(\ \frac{1}{x}\ \right)$$

An algebraic number $\alpha \neq 1$ is said to be *reciprocal* if $m_{\alpha,\mathbb{Z}}(x)$ is reciprocal. This is equivalent to $1/\alpha$ being a Galois conjugate of α.

One of the first results in response to Lehmer's problem was that of R. Breusch [Bre51]. He proved that if $f \;\in\; \mathbb{Z}[x]$ is irreducible, monic and non-reciprocal then $\mathrm{M}(f) > 1.179$. This was a significant result for if α is an algebraic number such that $[\mathbb{Q}(\alpha):\mathbb{Q}]$ is odd then

$$m_{\alpha,\mathbb{Z}}(x) \;\neq\; \left(\ \pm x^{[\mathbb{Q}(\alpha):\mathbb{Q}]}\ \right) \cdot m_{\alpha,\mathbb{Z}}\left(\ \frac{1}{x}\ \right)$$

and $\mathrm{M}(\alpha) > 1.179 > \mathrm{M}(l)$. Breusch was not able to identify the lowest non-reciprocal Mahler measure. This was accomplished by C. Smyth [Smy71]. We record his result as a theorem

Theorem 3.3.1. (Smyth) *Let α be a nonzero and nonreciprocal algebraic number then*

$$\mathrm{M}(\alpha) \geq x^3 - x - 1 \tag{3.3.1}$$

with equality only for $\pm\alpha^k$ a the root of the irreducible and non-reciprocal polynomial $x^3 - x - 1$, $k \geq 1$.

3.4 Lengths, Discriminants and Derivatives

In this section, we describe three results of Mahler that were established in the early 1960's. They represent some of the first progress towards a resolution of Lehmer's problem since the 1951 result of R. Breusch [Bre51]. In 1960 [Mah60] Mahler established the following.

Theorem 3.4.1. (Mahler) *Let $d \in \mathbb{N}$ and $a_0, \ldots, a_d \in \mathbb{Z}$ such that $a_0 \neq 0$ and $a_d \neq 0$. Let $f \in \mathbb{Z}[x]$ be given by*

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-1} x + a_d$$

Let $||\cdot||_\infty$ *be the usual archimedean absolute value on* $\mathbb{C}$. *Let*

$$\mathrm{L}(f) \;=\; \big|\big|a_0\big|\big|_\infty \;+\; \cdots \;+\; \big|\big|a_d\big|\big|_\infty$$

Then

$$2^{-d} \cdot \mathrm{L}(f) \;\leq\; \mathrm{M}(f) \;\leq\; \mathrm{L}(f) \tag{3.4.1}$$

Proof. Mahler's proof of inequality (3.4.1) is easy and worth providing here. To this end, let $\xi_1, \ \ldots, \ \xi_d$ be the roots of f and let $\mathcal{P}_d$ denote the set of all nonempty subsets of $\{\ 1, \ \ldots, \ d\ \}$. Since $a_d \neq 0$ these roots are all nonzero. We can suppose, without a loss of generality, that there exists $N \ \in \ \{\ 1, \ \ldots, \ d\ \}$ such that

$$||\xi_1||_\infty \leq ||\xi_2||_\infty \leq \cdots \leq ||\xi_N||_\infty \leq 1 < ||\xi_{N+1}||_\infty \leq \cdots \leq ||\xi_d||_\infty \tag{3.4.2}$$

Let $\mathcal{S} \ \in \ \mathcal{P}_d$. From inequality (3.4.2) it follows that

$$\left|\left|a_0 \prod_{v \in \mathcal{S}} \xi_v\right|\right|_\infty \;\leq\; ||a_0||_\infty \cdot \left|\left|\prod_{i=N+1}^{d} \xi_i\right|\right|_\infty \tag{3.4.3}$$

By equation (3.1.2) this is equivalent to

$$\left|\left|a_0 \prod_{v \in \mathcal{S}} \xi_v\right|\right|_\infty \;\leq\; \mathrm{M}(f) \tag{3.4.4}$$

For $i \in \{\ 1, \ \ldots, \ d\ \}$, each coefficient a_i of f is a sum of $\binom{d}{i}$ terms of the form

$$a_0 \xi_{i_1} \xi_{i_2} \cdots \xi_{i_m} \tag{3.4.5}$$

where the summation extends over all elements of $\mathcal{P}_d$ of order i.

In particular

$$\mathrm{L}(f) \;\leq\; \big|\big|a_0\big|\big|_\infty \cdot \sum_{\mathcal{S}\in\mathcal{P}_d} \left|\left| \prod_{v\in\mathcal{S}} \xi_v \right|\right|_\infty \tag{3.4.6}$$

Since

$$\sum_{i=0}^{d} \left(\begin{array}{c} d \\ i \end{array} \right) \;=\; 2^d \tag{3.4.7}$$

it follows that

$$\mathrm{L}(f) \;\leq\; 2^d \cdot \mathrm{M}(f) \tag{3.4.8}$$

For $z \in \mathbb{C}$ such that $||z||_\infty = 1$, it follows from the triangle inequality that

$$\big|\big|f(z)\big|\big|_\infty \;\leq\; \mathrm{L}(f)$$

As a result, by equation (3.1.1), $\mathrm{M}(f) \leq \mathrm{L}(f)$. $\square$

Corollary 3.4.2. (Polynomials of Bounded Measure and Degree) *Let $D \in \mathbb{N}$ and $T \in \mathbb{R}$, $T > 1$. Then there exist finitely many polynomials $f \in \mathbb{Z}[x]$ of degree $\leq D$ and $\mathrm{M}(f) < T$.*

In 1961 [Mah61] Mahler established the following.

Theorem 3.4.3. (Mahler) *Let $d \in \mathbb{N}$ and let $f \in \mathbb{Z}[x]$ be of degree d. Let f' be*

the derivative of f. Then

$$\mathrm{M}(f') \ \leq \ d \cdot \mathrm{M}(f) \tag{3.4.9}$$

Mahler's proof of Theorem 3.4.3 is lengthy and hence not included here.

In a different direction, let $d \in \mathbb{N}$ and let $a_0, \ \ldots \ , \ a_d \in \mathbb{Z}$ be such that $a_0 \neq 0$ and $a_d \neq 0$. Let $f(x) = a_0 x^d + \cdots + a_1 x + a_0 \ \in \ \mathbb{Z}[x]$. Let $\alpha_1, \ \ldots \ , \ \alpha_d$ be the roots of $f(x)$. The discriminant of $f(x)$, denoted $\mathrm{D}(f)$, is defined as

$$\mathrm{D}(f) \ = \ a_0^{2d-2} \cdot \prod_{1 \leq j < k \leq d} (\alpha_k - \alpha_j)^2 \tag{3.4.10}$$

In 1964 [Mah64] Mahler proved the following

Theorem 3.4.4. (Mahler) *Let $d \in \mathbb{N}, \ d \geq 2$ and $a_0, \ \ldots \ , \ a_d \in \mathbb{Z}$ such that $a_0 \neq 0$ and $a_d \neq 0$. Let $|| \cdot ||_\infty$ be the usual archimedean absolute value on $\mathbb{C}$. For a polynomial $f(x) = a_0 x^d + \cdots + a_{d-1} x + a_d \ \in \ \mathbb{Z}[x]$,*

$$\Big|\Big|\mathrm{D}(f)\Big|\Big|_\infty \ \leq \ \Big(\ d^d \ \Big) \cdot \Big(\ \mathrm{M}(f)^{2d-2} \ \Big) \tag{3.4.11}$$

with equality if and only if f has the form

$$f(x) = a_0 x^d + a_d, \quad \textit{where} \ \ \big|\big|a_0\big|\big|_\infty = \big|\big|a_d\big|\big|_\infty \ > 0 \tag{3.4.12}$$

3.5 Unconditional Lower Bounds

From Corollary 3.4.2, we know that if $(\alpha_i)_{i\in\mathbb{N}}$ is a sequence in $\overline{\mathbb{Q}}^\times - \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ )$ such that $\mathrm{M}(\alpha_i) \longrightarrow 1$ as $i \longrightarrow \infty$ then $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] \longrightarrow \infty$ as $i \longrightarrow \infty$. Bounds for the Mahler measure of algebraic numbers that depend only on the degree over $\mathbb{Q}$ are called *unconditional bounds.*

Let $\alpha \in \overline{\mathbb{Q}}^\times - \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ )$ and $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. In 1971, Blanksby and Montgomery [Bla71] proved that $\mathrm{M}(\alpha) > 1 + 1/(2d\log(6d))$. In 1978, C. L. Stewart [Ste78] used different methods to show that $\mathrm{M}(\alpha) > 1 + 1/(10^4 d\log d)$. Stewart's result is weaker than that of Blanksby and Montgomery, but E. Dobrowolski [Dob79] improved on Stewart's methods to show that for each $\epsilon > 0$ there exists $n(\epsilon)$ such that for $d > n(\epsilon)$,

$$\mathrm{M}(\alpha) > 1 + 1 - \epsilon\left(\ \frac{\log\log d}{\log d}\ \right)^3 \tag{3.5.1}$$

and that for $d \geq 3$

$$\mathrm{M}(\alpha) > 1 + \frac{1}{1200}\left(\ \frac{\log\log d}{\log d}\ \right)^3 \tag{3.5.2}$$

In 1982, D. C. Cantor and E. G. Strauss [Can82] were able to simplify Dobrowolski's proof and were able to improve the constant in inequality (3.5.1) to $2-\epsilon$. In 1983, R. Louboutin [Lou83] further improved the constant in inequality (3.5.1) to $9/4 - \epsilon$.

Theorem 3.5.1. (Louboutin) *Let* $\alpha \in \overline{\mathbb{Q}}^\times - \mathrm{Tor}(\ \overline{\mathbb{Q}}^\times\ )$ *and* $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. *For* $\epsilon > 0$ *there exists* $n(\epsilon)$ *such that if* $d > n(\epsilon)$ *then*

$$\mathrm{M}(\alpha) > 1 + 9/4 - \epsilon\left(\ \frac{\log\log d}{\log d}\ \right)^3 \tag{3.5.3}$$

We note that P. Voutier [Vou96] has established that

$$\log \mathrm{M}(\alpha) \ > \frac{1}{4} \cdot \left(\ \frac{\log \log d}{\log d} \ \right)^3 \tag{3.5.4}$$

This result is weaker asymptotically than inequality (3.5.3) but does not require that $d > n(\epsilon)$.

3.6 Bounds Based on Algebraic Properties

In the absence of a resolution to Lehmer's Problem we are motivated to pursue *conditional* lower bounds on the Mahler measure of algebraic numbers different from zero and the roots of unity. In this pursuit, we are allowed by equation (3.1.2) to assume that α is an algebraic integer.

Theorem 3.6.1. (Garza) *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension. Let $\mathrm{Z}_{\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )}$ be the center of $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $n = [\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) : \mathrm{Z}_{\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )}]$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\ \mathcal{O}_{\mathbb{K}}^{\times}\ )$ be such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. Let $a \in (1, \infty)$. Let*

$$\mathrm{H}_n \equiv \frac{2^{1-n} + \sqrt{4^{1-n} + 4}}{2}$$

If

$$[\mathbb{K} : \mathbb{Q}] \ \geq \ \frac{2 \cdot n^2 \cdot \log a}{\log \mathrm{H}_n}$$

Then

$$\mathrm{M}(\alpha) \geq a$$

Proof. Let $\mathrm{G} = \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ )$. Let $\mathrm{H}_{\mathbb{Q}(\alpha)}$ be the subgroup of G that fixes the field $\mathbb{Q}(\alpha)$. From Galois theory we know that $\mathrm{Z_G} \bigcap \mathrm{H}_{\mathbb{Q}(\alpha)} = \{1\}$ from which it follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq |\mathrm{G}|/n$. By Theorem 2.4.2 we have that $h(\alpha) \geq \log \mathrm{H}_n^{1/(2 \cdot n)}$. If $[\mathbb{K} : \mathbb{Q}] = |\mathrm{G}| \geq (2 \cdot n^2 \cdot \log a)/\log \mathrm{H}_n$ then, by Lemma 3.1.2, we have $\mathrm{M}(\alpha) \geq a$ $\square$.

Among other things, Theorem 3.6.1 shows that if $(\alpha_i)_{i \in \mathbb{N}}$ is a sequence of $\overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$ such that $\mathrm{M}(\alpha_i) \longrightarrow 1$ as $i \longrightarrow \infty$, then the index of the center of the Galois group of the Galois closure of $\mathbb{Q}(\alpha_i) \longrightarrow \infty$.

It follows from Theorem 2.3.1 and equation (3.1.23) that if α is an algebraic integer different from zero and the roots of unity such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is an abelian extension then $\mathrm{M}(\alpha) \geq \mathrm{H}_0$. This consequence of Theorem 2.3.1, restricted to algebraic integers, is contained within Theorem 3.6.1 with $n = 1$ and $a = (1 + \sqrt{5})/2$.

Although Theorem 3.6.1 is conditional in it's hypothesis, the condition imposed is amongst the most natural possible. Moreover, although the condition is stated in terms of the Galois group of the Galois closure of $\mathbb{Q}(\alpha)$, it follows from Theorem 2.4.1 and equation (3.1.24) that we can equivalently state our Theorem as depending on the fraction of Galois conjugates of α that can be simultaneously embedded into the real numbers.

3.7 Extremal Polynomials

Let $\mathbb{K}/\mathbb{Q}$ be a finite extension and define

$$\lambda_{\mathbb{K}} \ = \ \inf \left\{ \ \mathrm{M}(\alpha) \ : \ \alpha \in \mathbb{K}^{\times} - \mathrm{Tor}(\ \mathbb{K}^{\times}\ ) \ \right\}$$

It follows from Corollary 3.4.2 that there exist $\beta \in \mathbb{K}^\times - \mathrm{Tor}(\ \mathbb{K}^\times\ )$ such that $\mathrm{M}(\beta) = \lambda_{\mathbb{K}}$. Define

$$\mathcal{E}_{\mathbb{K}} \equiv \left\{\ \beta \in \mathbb{K}^\times - \mathrm{Tor}(\ \mathbb{K}^\times\ )\ :\ \mathrm{M}(\beta) = \lambda_{\mathbb{K}}\ \right\}$$

If $\gamma \in \mathcal{E}_{\mathbb{K}}$ such that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = \min\{\ [\mathbb{Q}(\beta) : \mathbb{Q}]\ :\ \beta \in \mathcal{E}_{\mathbb{K}}\ \}$ then we will say that γ is *extremal* for the Mahler measure in $\mathbb{K}$. The following lemma is due to J.Vaaler [Val07] and is of importance when implementing Lemmas 2.5.5 and 2.5.6.

Lemma 3.7.1. (Vaaler) *Let $\mathbb{K}/\mathbb{Q}$ be a finite extension. Let $\alpha \in \mathbb{K}^\times - \mathrm{Tor}(\ \mathbb{K}^\times\ )$ be extremal for the Mahler measure in $\mathbb{K}^\times - \mathrm{Tor}(\ \mathbb{K}^\times\ )$. Then for all $s \in \mathbb{N}$, $\mathbb{Q}(\alpha^s) = \mathbb{Q}(\alpha)$.*

Proof. Suppose $\exists\ s \in \mathbb{N},\ s \geq 2$ such that $[\mathbb{Q}(\alpha^s) : \mathbb{Q}] < [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and let ζ_s be a fixed primitive $s-th$ root of unity. Let $m_{\alpha,\mathbb{Q}(\alpha^s)}(x)$ be the minimal polynomial of α over the field $\mathbb{Q}(\alpha^s)$. Since α is a root of $x^s - \alpha^s \in \mathbb{Q}(\alpha^s)[x]$, we have that $m_{\alpha,\mathbb{Q}(\alpha^s)}(x)$ is a divisor of

$$x^s - \alpha^s\ =\ \prod_{m=1}^{s}(x - \zeta_s^m \cdot \alpha)$$

there thus exists $\mathcal{L} \subseteq \{\ 1,\ \ldots,\ s\ \}$ such that

$$m_{\alpha,\mathbb{Q}(\alpha^s)}(x)\ =\ \prod_{l\in\mathcal{L}}(x - \zeta_s^l\alpha)$$

We have that $|\mathcal{L}| = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^s)] = r$. Let $L = \sum_{l\in\mathcal{L}} l$. Then

$$\beta \;\equiv\; (-1)^r \cdot m_{\alpha,\mathbb{Q}(\alpha^s)}(0) \;=\; \zeta_s^L \alpha^r \in \mathbb{Q}(\alpha^s)$$

and so $h(\beta) \;=\; r \cdot h(\alpha)$ and

$$\begin{aligned}
\log \mathrm{M}(\beta) &= [\mathbb{Q}(\beta) : \mathbb{Q}] \cdot h(\beta) \\
&\leq [\mathbb{Q}(\alpha^s) : \mathbb{Q}] \cdot h(\beta) \\
&= [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^s)] \cdot [\mathbb{Q}(\alpha^s) : \mathbb{Q}] \cdot h(\alpha) \\
&= [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha) \\
&= \log \mathrm{M}(\alpha)
\end{aligned}$$

Since $[\mathbb{Q}(\beta) : \mathbb{Q}] < [\mathbb{Q}(\alpha) : \mathbb{Q}]$, this contradicts our assumption that α is extremal for the Mahler measure in $\mathbb{K}^\times - \mathrm{Tor}(\ \mathbb{K}^\times\ )$. It follows that $\mathbb{Q}(\alpha^s) = \mathbb{Q}$. $\square$

Chapter 4

Dihedral Extensions

4.1 Introduction

Let $m \in \mathbb{N},\ m \geq 3$. In this section, $D_{2\cdot m}$ will be a group with presentation

$$D_{2\cdot m} = \langle\ \sigma,\ \tau \mid \tau^2 = \sigma^m = 1,\ \tau\sigma\tau = \sigma^{-1}\ \rangle \tag{4.1.1}$$

and we say that a group G is *dihedral* if there exists $m \in \mathbb{N},\ m \geq 3$ such that $\mathrm{G} \approx D_{2\cdot m}$. As a way of extending Section 3.6 we ask if there exists a constant $C_D > 1$ such that for all $\alpha \in \overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$, contained in dihedral Galois extensions of $\mathbb{Q}$, $\mathrm{M}(\alpha) \geq C_D$. We will demostrate that the answer is yes and that $C_D = \mathrm{M}(x^3 - x - 1)$ is the best possible such constant. Our ability to answer this question in the affirmative leads to the construction of new research problems.

Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension such that there exists $m \in \mathbb{N},\ m \geq 3$ for which $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx D_{2\cdot m}$. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. From Theorem 2.4.2 and Lemma 3.1.2 we can suppose that $\xi \notin \mathrm{Z_G}$. In this case we can also show that

$|\mathrm{Z_G}(\xi)| \in \{ 2, 4 \}$ so that the archimedean estimates of Theorem 2.4.2 are not useful.

It follows from Theorem 3.3.1 and equation (3.1.2) that we may suppose $\alpha \in \mathbb{K}$ to be a reciprocal algebraic integer. It follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even and that for all non-archimedean places v of $\mathbb{K}$, $|\alpha|_v = 1$.

4.2 Orders not Divisible by 4

As a necessary and simplifying preliminary step, dihedral extensions of degrees not divisible by 4 are considered first. Let $m \in \mathbb{N}$, $m \geq 3$. The distinct elements of $\langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot m}$ are $1, \sigma, \sigma^2, \ldots, \sigma^{m-1}, \tau, \sigma\tau, \ldots, \sigma^{m-1}\tau$. Consequently, if a subgroup, H, of a dihedral group, $\langle\sigma\rangle \rtimes_\rho \langle\tau\rangle$, is of order 3 or larger, then $\mathrm{H} \bigcap \langle\sigma\rangle \neq \{1\}$.

Lemma 4.2.1. (Algebraic Integers of Degree 2) *Let α be an algebraic integer (different from the roots of 1) of degree 2 over $\mathbb{Q}$. Then $\mathrm{M}(x^3 - x - 1) \leq \mathrm{M}(\alpha)$.*

Proof. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ we have that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is abelian so that the Lemma follows from Theorem 3.6.1 with $n = 1$ and $a = \mathrm{M}(x^3 - x - 1)$. □

Lemma 4.2.2. (Quotients of Dihedral Groups) *Let $m \in \mathbb{N}$, $m \geq 3$ and let*

$$\mathrm{G} = \langle\sigma\rangle \rtimes_\phi \langle\tau\rangle \approx D_{2\cdot m}$$

Suppose that m is composite and that $j \in \mathbb{N},\ 1 < j < m$ is a divisor of m. Then

$$\mathrm{G} \ / \ \langle \sigma^j \rangle \ \approx \ \begin{cases} D_{2 \cdot j} & \text{if } \ j \neq 2 \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & \text{if } \ j = 2 \end{cases}$$

Proof. $\langle \sigma \rangle \ \trianglelefteq \ \mathrm{G}$ and $\langle \sigma \rangle$ is cyclic. Subgroups of cyclic groups are characteristic. Characteristic subgroups of normal subgroups are normal. Thus $\langle \sigma^j \rangle \ \trianglelefteq \ \mathrm{G}$. $|\langle \sigma^j \rangle| = m/j$. Therefore, $[\mathrm{G} : \langle \sigma^j \rangle] = 2j$. Let $\rho : \mathrm{G} \to \mathrm{G}/\langle \sigma^j \rangle$ be the natural projection homomorphism. Then $Im(\rho) \approx \mathrm{G}/\langle \sigma^j \rangle$ and $Im(\rho) = \langle \rho(\tau), \rho(\sigma) \rangle$. $\sigma\tau = \tau\sigma^{-1}$ implies that $\rho(\sigma)\rho(\tau) = \rho(\tau)(\rho(\sigma))^{-1}$. We have $|\rho(\tau)| = 2$ and $|\rho(\sigma)| = j$, so there exists a presentation for $Im(\rho)$ identical to that for $D_{2 \cdot j}$ or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ depending on wether $j \neq 2$ or $j = 2$ $\square$

Lemma 4.2.3. (Primitive Elements in Galois Extensions) *Let $\mathbb{K}/\mathbb{Q}$ be a nonabelian, not totally real, finite Galois extension. Let $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\ \mathcal{O}_{\mathbb{K}}^{\times}\ )$ be a primitive element. Then α is not extremal for the Mahler measure in $\mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\ \mathcal{O}_{\mathbb{K}}^{\times}\ )$.*

Proof. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \ \in \ \mathrm{G} = \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ correspond to complex conjugation with respect to η. By Lemma 3.2.1, we can assume that $||\alpha||_{\infty} \neq 1$ with respect to η. Let $\beta \equiv \alpha \cdot \xi(\alpha)$. From inequality (2.2.10), $h(\beta) \leq 2 \cdot h(\alpha)$. Since $\mathbb{K}$ is not totally real, $[\mathbb{K} : \mathbb{Q}(\beta)] \geq 2$. Thus

$$[\mathbb{Q}(\beta) : \mathbb{Q}] \cdot h(\beta) \leq 2 \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] \cdot h(\alpha) \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha)$$

and, by Lemma 3.1.2, $\mathrm{M}(\beta) \leq \mathrm{M}(\alpha)$ $\square$

Lemma 4.2.4. (Galois Extensions of $\mathbb{Q}$ of Degree 2p) *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension of degree $2 \cdot p$, where p is a rational prime. If $\alpha \in \mathbb{K}^{\times} - \mathrm{Tor}(\ \mathbb{K}^{\times}\ )$ then $\mathrm{M}(x^3 - x - 1) \ \leq \ \mathrm{M}(\alpha)$.*

Proof. By Lemma 4.2.3, Theorem 2.3.1 and Lemma 3.1.2 we can assume that $d \equiv [\mathbb{Q}(\alpha) : \mathbb{Q}] \in \{\ 1,\ 2,\ p\ \}$. If $d = 1$ then $\alpha \in \mathbb{Z}$ and so $h(\alpha) \geq \log 2$. If $d = 2$, then by Lemma 4.2.1, $\mathrm{M}(x^3 - x - 1) \ \leq \ \mathrm{M}(\alpha)$. If $d = p$ and $p \neq 2$, then, by the Theorem 3.3.1, $\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$. So, in all the possible cases, $\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$. □

Proposition 4.2.5. (Dihedral Galois Groups not Divisible by 4) *Let $m \in \mathbb{N}$ such that m is odd and $m \geq 3$. Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with*

$$\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle \sigma \rangle \rtimes_{\phi} \langle \tau \rangle \approx D_{2 \cdot m}$$

If $\alpha \in \mathbb{K}^{\times} - \mathrm{Tor}(\ \mathbb{K}^{\times}\ )$, then $\mathrm{M}(x^3 - x - 1) \ \leq \ \mathrm{M}(\alpha)$.

Proof. By Theorem 2.3.1 and Lemma 3.1.2 we may suppose that $\mathbb{K}$ is not totally real. The proof will be by induction on the number of prime factors, including multiplicity, of $2 \cdot m$. By Lemma 4.2.4, Proposition 4.2.5. is true in the case where m is a prime number.

Let n be the number of prime factors, including multiplicity of $2 \cdot m$. Assume that for all $l \in \mathbb{N},\ l \geq 3$ such that $2 \cdot l$ has less than n prime factors including multiplicity, that if $\mathbb{F}/\mathbb{Q}$ is a Galois extension such that $\mathrm{Aut}(\ \mathbb{F}/\mathbb{Q}\ ) \approx D_{2 \cdot l}$ and $\gamma \in \mathbb{F}^{\times} - \mathrm{Tor}(\ \mathbb{F}^{\times}\ )$, then $\mathrm{M}(\gamma) \geq \mathrm{M}(x^3 - x - 1)$.

By Lemma 4.2.3, we can assume that α is not a primitive element. If

$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is odd then, by Theorem 3.3.1, $\mathrm{M}(x^3 - x - 1) \leq \mathrm{M}(\alpha)$.

If $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even, then the subgroup of G fixing the field $\mathbb{Q}(\alpha)$ contains a nontrivial subgroup of $\langle\sigma\rangle$. So, by Lemma 4.2.2, $\alpha \in \mathbb{V}$ where $\mathbb{V}$ is either a dihedral Galois extension of $\mathbb{Q}$ of order containing less than n prime factors or is abelian. Hence, by the induction hypothesis, $\mathrm{M}(x^3 - x - 1) \leq \mathrm{M}(\alpha)$. $\square$

Let $\mathbb{K}$ be the splitting field of the polynomial $f(x) = x^3 - x - 1$. Then $\mathbb{K}/\mathbb{Q}$ is a Galois extension and $[\mathbb{K} : \mathbb{Q}] \in \{\ 3,\ 6\ \}$. The discriminant of $f(x)$ is -23. As a result, $(-23)^{1/2} \in \mathbb{K}$. $[\mathbb{Q}(-23)^{1/2} : \mathbb{Q}] = 2$ so that $2 \mid [\mathbb{K} : \mathbb{Q}]$ and thus $[\mathbb{K} : \mathbb{Q}] = 6$. Consequently, $\mathrm{Aut}\big(\ \mathbb{K}/\mathbb{Q}\ \big) \approx \mathrm{S}_3 \approx D_{2\cdot 3}$. We thus know, by Proposition 4.2.5, that amongst all polynomials in $\mathbb{Z}[x]$ whose splitting fields are contained in dihedral Galois extensions of $\mathbb{Q}$ of degree not divisible by 4, $x^3 - x - 1$ has the smallest Mahler measure (other than 1).

4.3 Subgroups of Dihedral Groups

By Proposition 4.2.5, we may restrict to consideration of dihedral Galois groups of orders divisible by four. The subgroups of such groups will be of importance and the purpose of this section is to identify relevant properties of these subgroups. It will be helpfull to keep in mind, that if $m \in \mathbb{N},\ m \geq 3$, then, as a set

$$D_{2\cdot m} \approx \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle = \{\ 1,\ \sigma,\ \sigma^2,\ \ldots,\ \sigma^{m-1},\ \tau,\ \sigma\tau,\ \ldots,\ \sigma^{m-1}\tau\ \}$$

Lemma 4.3.1. (Elements of order 2) *Let* $m \in \mathbb{N},\ m \geq 2$. *Let* $\mathrm{G} = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot 2m}$. *The elements of order* 2 *in* G *are* $\sigma^i\tau$ *for* $i \in \{\ 0,\ \ldots,\ 2m-1\ \}$ *and* σ^m.

Proof. $\forall\ i\ \in \{\ 1,\ \ldots,\ 2m-1\ \}$ we have $|\sigma^i| = 2m/(2m,i) = 2$ if and only if $i = m$. Thus, the only power of σ of order 2 is σ^m. Let $j \in \{\ 0,\ \ldots,\ 2m-1\ \}$ then $\sigma^j\tau \cdot \sigma^j\tau = \sigma^j\sigma^{-j}\tau\tau = 1$. So that $|\sigma^j\tau| = 2$. Since all elements of G have been considered, the proof of Lemma 4.3.1 is complete. $\square$

Lemma 4.3.2. ($\mathbf{N_G}(\sigma^i\tau)$) *Let* $m \in \mathbb{N},\ m \geq 2$. *Let* $\mathrm{G} = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot 2m}$. *Let* $i \in \{\ 0,\ \ldots,\ 2m-1\ \}$. *Then* $\mathrm{N_G}(\langle\sigma^i\tau\rangle) = \langle\sigma^i\tau, \sigma^m\rangle$.

Proof. Let $j \in \{\ \ 1,\ \ldots,\ 2m-1\ \}$. $\sigma^j(\sigma^i\tau)\sigma^{-j} = \sigma^j\sigma^j(\sigma^i\tau) = \sigma^{2j}(\sigma^i\tau) = \sigma^i\tau$ if and only if $\sigma^{2j} = 1$ if and only if $j = m$. Thus $\langle\sigma^m, \sigma^i\tau\rangle \leq \mathrm{N_G}(\langle\sigma^i\tau\rangle)$. Similarly, for $s \in \{\ 0,\ \ldots,\ 2m-1\ \}$ we have $\sigma^s\tau(\sigma^i\tau)\sigma^s\tau = \sigma^{2s}(\sigma^{-i}\tau) = \sigma^i\tau$ if and only if $\sigma^{2s} = \sigma^{2i}$ if and only if $s = m+i$ or $s = i$. Therefore, since all elements of G have been considered, $\mathrm{N_G}(\langle\sigma^i\tau\rangle) = \langle\sigma^m, \sigma^i\tau\rangle$. $\square$

Let $m \in \mathbb{N},\ m \geq 2$ and let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx D_{2\cdot 2m}$. Let $\eta :\ \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. It follows from Lemmas 4.3.1 and 4.3.2. that either $[\mathrm{G} : \mathrm{Z_G}(\xi)] = 1$ or $[\mathrm{G} : \mathrm{Z_G}(\xi)] = m$. Since we are supposing that $\xi \notin \mathrm{Z_G}$ it follows that $[\mathrm{G} : \mathrm{Z_G}(\xi)] = m$ so that Theorem 2.4.2 is not of use.

Lemma 4.3.3. (Cyclic Subgroups) *Let* $m \in \mathbb{N},\ m \geq 2$. *Let* $\mathrm{G} = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot 2m}$. *The cyclic subgroups of* G *are* $\langle\sigma^i\rangle$ *for* $i\ \in\ \mathbb{N}$ *a divisor of* $2m$ *and* $\langle\sigma^i\tau\rangle$ *for* $i \in \{\ 0,\ \ldots,\ 2m-1\ \}$. *For all* $\mathrm{H}\ \leq\ \langle\sigma\rangle$, *we have* $\mathrm{H}\ \trianglelefteq\ \mathrm{G}$.

Proof. Let K be a cyclic subgroup of G. Suppose that there exists $i \in \{ 0, \ldots, 2m-1 \}$ such that $\langle \sigma^i\tau \rangle \lhd$ K. By Lemma 4.3.2. $\mathrm{N_G}(\langle \sigma^i\tau \rangle) = \langle \sigma^m, \sigma^i\tau \rangle \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so that we have $\mathrm{K} = \langle \sigma^i\tau \rangle$. Since all the elements of G have been considered, we have found all the cyclic subgroups of G. $\langle \sigma \rangle$ is characteristic in G and subgroups of a cyclic group are characteristic. Characteristic subgroups of a characteristic subgroup are themselves characteristic. So that if $\mathrm{K} \lhd \langle \sigma \rangle$ then $\mathrm{K} \lhd \mathrm{G}$. $\square$

Lemma 4.3.4. (The Commutator and the Center) *Let* $m \in \mathbb{N},\ m \geq 3$ *and* $\mathrm{G} = \langle \sigma \rangle \rtimes_\rho \langle \tau \rangle \approx D_{2\cdot m}$. *The the commutator subgroup of* G *is* $\langle \sigma^2 \rangle$. *If* m *is even, then* $\mathrm{Z_G} = \langle \sigma^{m/2} \rangle$.

Proof. $\mathrm{G} = \langle \sigma, \tau \mid \sigma^m = \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1} \rangle$. Let G' denote the commutator subgroup of G. $[\sigma, \tau] = \sigma^{-2}$ so $\langle \sigma^{-2} \rangle = \langle \sigma^2 \rangle \leq \mathrm{G}'$. $\langle \sigma^2 \rangle \trianglelefteq$ G. Let $\phi : \mathrm{G} \to \mathrm{G}/\langle \sigma^2 \rangle$ be the natural projection homomorphism. Then, if m is even, $|\phi(\sigma)| = 2$ and if m is odd $|\phi(\sigma)| = 1$. So that $\phi(\sigma)^{-1} = \phi(\sigma)$. If m is even, we have

$$\phi(\mathrm{G}) \ = \ \langle\ \phi(\sigma),\ \phi(\tau) \mid \phi(\sigma)^2 = \phi(\tau)^2 = 1,\ \phi(\tau)\phi(\sigma)\phi(\tau) = \phi(\sigma)\ \rangle$$

So that $\phi(\mathrm{G}) \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If m is odd, we have

$$\phi(\mathrm{G}) = \langle \phi(\sigma), \phi(\tau) \mid \phi(\sigma) = \phi(\tau)^2 = 1 \rangle$$

So that $\phi(\mathrm{G}) \approx \mathbb{Z}/2\mathbb{Z}$. In either case, we have, by the universal property of the commutator subgroup, that $\mathrm{G}' \leq \langle \sigma^2 \rangle$ so that $\mathrm{G}' = \langle \sigma^2 \rangle$.

If m is even, then $(\sigma^{m/2})^{-1} = \sigma^{m/2}$ and consequently $\tau\sigma^{m/2} = \sigma^{m/2}\tau$ from which it follows that $\sigma^{m/2} \in \mathrm{Z_G}$. If $i \in \{ 0, \ldots, m-1 \}$ and $i \neq m/2$. Then

$\sigma^i \neq \sigma^{-i}$ so that $\tau\sigma^i \neq \sigma^i\tau$ and consequently $\sigma^i \notin \mathrm{Z_G}$. By Lemma 4.3.2, we have that, for all $i \in \{ 0, \ldots, m-1 \}$, $\sigma^i\tau \notin \mathrm{Z_G}$. Since all the elements of G have been considered, $\mathrm{Z_G} = \langle \sigma^{m/2} \rangle$. $\square$

Lemma 4.3.5. (nth Roots of Unity in Dihedral Extensions) *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension with dihedral Galois group. For $q \geq 5$, q a rational prime, the primitive qth roots of unity are not in $\mathbb{K}$. The primtive 9th roots of unity are not in $\mathbb{K}$.*

Proof. Let ϕ be the Euler function. For $m \in \mathbb{N}$ let ζ_m be a primitive $m-th$ root of unity. Then $\mathrm{Aut}\big(\mathbb{Q}(\zeta_q) \,/\, \mathbb{Q} \big) \approx \mathbb{Z}/\phi(q)\mathbb{Z}$. By Lemma 4.3.4, and The Fundamental Theorem of Galois Theory, the maximal abelian subfield of $\mathbb{K}$ has Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ so that $\zeta_q \notin \mathbb{K}$ and $\zeta_9 \notin \mathbb{K}$. $\square$

Lemma 4.3.6. (Sylow-2 Subgroups of Inertia Groups) *Let $m \in \mathbb{N}$, $m \geq 2$. Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension such that* $\mathrm{Aut}(\, \mathbb{K}/\mathbb{Q} \,) \approx D_{2\cdot(2m)}$. *Let $p \geq 3$ be a rational prime and let v be a place of $\mathbb{K}$ restricting to the $p-$adic place of $\mathbb{Q}$. Let* $\mathrm{G_0}$ *be the inertia group of v. Let* H *be a Sylow-2 subgroup of* $\mathrm{G_0}$ *and let* K *be a Sylow-2 subgroup of* G *containing* H. *Then* $[\mathrm{K} : \mathrm{H}] \geq 2$.

Proof. Let G' denote the commutator subgroup of G. Let $\mathbb{F}_{\mathrm{G}'}$ be the subfield of $\mathbb{K}$ fixed by G'. By Lemma 4.3.4, and Galois correspondence, there exists relatively prime rational integers D_1 and D_2 such that $\mathbb{F}_{\mathrm{G}'} = \mathbb{Q}(\, \sqrt{D_1}, \sqrt{D_2} \,)$. Consequently, we may assume that $p \nmid D_1$ in which case p does not ramify in $\mathbb{Q}(\, \sqrt{D_1} \,)$ (see Section 16.3 of [Dum99] exercise 22). It then follows, by the transistivity of the

ramification index, that $[\mathrm{K} : \mathrm{H}] \geq 2$. $\square$

Lemma 4.3.7. (Normalizers of Non-normal Subgroups) *Let* $m \in \mathbb{N},\ m \geq 2$ *and let* $\mathrm{G} = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot 2m}$. *Let* H be a non-normal subgroup of G. *Then* $[\mathrm{N_G(H)} : \mathrm{H}] \leq 2$. *If* $\mathrm{K} \leq \mathrm{G}$ *such that there exists* $i \in \{\ 0,\ \ldots,\ 2m-1\ \}$ *for which* $\sigma^i\tau \in \mathrm{K}$, *then* $[\mathrm{N_G(K)} : \mathrm{K}] \leq 2$.

Proof. By Lemma 4.3.3, $\exists\ i \in \{\ 0,\ \ldots,\ 2m-1\ \}$ such that $\sigma^i\tau \in \mathrm{H}$. Let $s \in \mathbb{N}$ such that $\langle\sigma^s\rangle = \langle\sigma\rangle \bigcap \mathrm{H}$. Then $\mathrm{H} = \langle\sigma^s\rangle \rtimes_\rho \langle\sigma^i\tau\rangle$. Suppose that $2 \mid [\langle\sigma\rangle : \langle\sigma^s\rangle]$, then since $[\langle\sigma\rangle : \langle\sigma^s\rangle] = (2m, s),\ \ 2 \mid s$. The elements of order 2 in H are $\sigma^{i+ts}\tau$ for $t \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$ and σ^m if $\sigma^m \in \mathrm{H}$. Let $r \in \{\ 0,\ \ldots,\ 2m-1\ \}$ and suppose that $\sigma^r\tau \in \mathrm{N_G(H)}$. Then, for all $t \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$, we have

$$\sigma^r\tau(\sigma^{ts+i}\tau)\sigma^r\tau = \sigma^{2r-(ts+i)}\tau \in \mathrm{H}$$

From which it follows that $\exists\ t' \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$ such that

$$\sigma^{2r-ts-i}\tau = \sigma^{t's+i}\tau$$

so that

$$\sigma^{2r} = \sigma^{(t+t')s+2i}$$

and

$$\sigma^r \in \sigma^i\langle\sigma^{s/2}\rangle$$

Let $n \in \{\ 1,\ \ldots,\ 2m-1\ \}$ such that $\sigma^n \in \mathrm{N_G(H)}$. Let $t \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$. Then, since $\sigma^{ts+i}\tau \in \mathrm{N_G(H)}$ so is $\sigma^{ts+n+i}\tau$ and consequently

$$\sigma^{ts+n+i} \in \sigma^i\langle\sigma^{s/2}\rangle$$

so that

$$\sigma^{ts+n} \in \langle\sigma^{s/2}\rangle$$

which implies that

$$\sigma^n \in \langle\sigma^{s/2}\rangle$$

Hence, we have that $\mathrm{N_G(H)} = \langle\sigma^{s/2}\rangle \rtimes_\rho \langle\sigma^i\tau\rangle$. So that $[\mathrm{N_G(H)} : \mathrm{H}] = 2$.

Suppose that $2 \nmid [\langle\sigma\rangle : \langle\sigma^s\rangle]$. Then since $[\langle\sigma\rangle : \langle\sigma^s\rangle] = (2m, s)$, $2 \nmid s$. The elements of order 2 in H are $\sigma^{i+ts}\tau$ for $t \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$ and σ^m (we note that, in this case, $\sigma^m \in \mathrm{H}$). Let $r \in \{\ 0,\ \ldots,\ 2m-1\ \}$ and suppose that $\sigma^r\tau \in \mathrm{N_G(H)}$. Then for all $t \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$ we have

$$\sigma^r\tau(\sigma^{ts+i}\tau)\sigma^r\tau = \sigma^{2r-(ts+i)}\tau \in \mathrm{H}$$

From which it follows that $\exists\ t' \in \{\ 0,\ \ldots,\ 2m/s-1\ \}$ such that

$$\sigma^{2r-ts-i}\tau = \sigma^{t's+i}\tau$$

so that

$$\sigma^{2r} = \sigma^{(t+t')s+2i}$$

and

$$\sigma^{2r} \in \sigma^{2i}\langle\sigma^s\rangle$$

Suppose that $\sigma^r \notin \sigma^i\langle\sigma^s\rangle$. Then $\sigma^{r-i} \notin \langle\sigma^s\rangle$, but $(\sigma^{r-i})^2 \in \langle\sigma^s\rangle$ which is a contradiction since $2 \nmid [\langle\sigma\rangle : \langle\sigma^s\rangle]$. Hence, we have that $\sigma^r \in \sigma^i\langle\sigma^s\rangle$ and consequently that $\sigma^r\tau \in \mathrm{H}$. Let $n \in \{ 1, \ldots, 2m-1 \}$ such that $\sigma^n \in \mathrm{N_G(H)}$. Let $t \in \{ 0, \ldots, 2m/s - 1 \}$. Then, since $\sigma^{ts+i}\tau \in \mathrm{N_G(H)}$ so is $\sigma^{ts+n+i}\tau$ and consequently

$$\sigma^{ts+n+i} \in \sigma^i\langle\sigma^s\rangle$$

so that

$$\sigma^{ts+n} \in \langle\sigma^s\rangle$$

which implies that $\sigma^n \in \langle\sigma^s\rangle$ and consequently that $\sigma^n \in \mathrm{H}$. It thus follows that $\mathrm{N_G(H)} = \mathrm{H}$ and consequently that $[\mathrm{N_G(H)} : \mathrm{H}] = 1$. $\square$

Lemma 4.3.8. (Order of a Stabilizer) *Let $m \in \mathbb{N}$, $m \geq 3$. Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx D_{2\cdot m}$. *Let p be a rational prime. Let v be a place of $\mathbb{K}$ restricting to the $p-$adic place of $\mathbb{Q}$. Let f be the residue class degree of v and e the ramification index of v. If $f \geq 3$ then $e \cdot f \leq m$.*

Proof. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle$. Let $\mathrm{G_0}$ be the inertia group of v and let Z_v be the decompositon group of v. By Theorem 1.9.1, $|\mathrm{G_0}| = e$, $\mathrm{G_0} \trianglelefteq \mathrm{Z}_v$, Z_v / $\mathrm{G_0}$ is cyclic, and $|\mathrm{Z}_v| = ef$. Since $[\mathrm{N_G(G_0)} : \mathrm{G_0}] \geq [\mathrm{Z}_v : \mathrm{G_0}] = f \geq 3$ it follows, by Lemma 4.3.7, that $\mathrm{G_0} \triangleleft \langle\sigma\rangle$. Suppose $\exists\ i \in \{ 0, \ldots, 2m-1 \}$ such that $\sigma^i\tau \in \mathrm{Z}_v$. Let $s \in N \bigcup \{0\}$ such that $\langle\sigma^s\rangle = \langle\sigma\rangle \bigcap \mathrm{Z}_v$. Then $\mathrm{Z}_v = \langle\sigma^s\rangle \rtimes_\rho \langle\sigma^i\tau\rangle$ and then, by Lemma 4.2.2, Z_v / $\mathrm{G_0}$ is not cyclic of order ≥ 3. This would be a contradiction. Consequently we have that $\mathrm{Z}_v \triangleleft \langle\sigma\rangle$. The result follows since $|\langle\sigma\rangle| = m$. $\square$

Lemma 4.3.9. (Normal Subgroups of Dihedral Groups) *Let* $m \in \mathbb{N},\ m \geq 3$. *Let* $\mathrm{G} = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot m}$. *Let* $\mathrm{H} \lhd \mathrm{G}$ *such that* $\mathrm{H} \not\trianglelefteq \langle\sigma\rangle$. *Then* $[\mathrm{G} : \mathrm{H}] = 2$ or $[\mathrm{G} : \mathrm{H}] = 1$.

Proof. By considering the distinct elements of G we have that there exists $i \in \{\ 0,\ \ldots,\ m-1\ \}$ such that $\sigma^i\tau \in \mathrm{H}$. By Lemma 4.3.7, $[\mathrm{N_G(H)} : \mathrm{H}] \leq 2$ and since $\mathrm{G} = \mathrm{N_G(H)}$, we have that $[\mathrm{G} : \mathrm{H}] \leq 2$. $\square$

Lemma 4.3.10. *Let* $m \in \mathbb{N},\ m \geq 2$. *Let* $\mathrm{G} = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot 2m}$. *Let* v *be a place of* $\mathbb{K}$ *that restricts to the 2-adic place on* $\mathbb{Q}$. *Let* $\mathrm{G_0}$ *be the inertia group of* v *and let* Z_v *be the stabilizer of* v. *If there exists* $i \in \{\ 0,\ \ldots,\ 2m-1\ \}$ *such that* $\sigma^i\tau \in \mathrm{G_0}$ *and* $\sigma^m \notin \mathrm{G_0}$ *then* $|\mathrm{G_0}| \in \{\ 2,\ 6\ \}$.

Proof. By Lemma 4.3.7, $[\mathrm{N_G(G_0)} : \mathrm{G_0}] \leq 2$. Since $\mathrm{G_0} \trianglelefteq \mathrm{Z}_v$ it follows that $|\mathrm{Z}_v\ /\ \mathrm{G_0}| = f \leq 2$. From Theorem 1.9.1, we have that the only possible odd divisors of $|\mathrm{G_0}|$ are 1 and 3. For $k,\ j \in \{\ 0,\ \ldots,\ 2m-1\ \}$, $(\tau\sigma^k)(\tau\sigma^j) \in \langle\sigma\rangle$ so that $\langle\tau\sigma^i\rangle \in \mathrm{Sylow_2(G_0)}$. $\square$

4.4 The Subgroup $\mathbf{H}_{\mathbb{Q}(\alpha)} \leq \mathbf{Aut}(\mathbb{K}/\mathbb{Q})$

Let $m \in \mathbb{N},\ m \geq 2$ and let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle \approx D_{2\cdot 2m}$. Let $\alpha \in \mathcal{O}_\mathbb{K}^\times - \mathrm{Tor}(\mathcal{O}_\mathbb{K}^\times)$ and let $\mathrm{H}_{\mathbb{Q}(\alpha)}$ be the subgroup of G that fixes the field $\mathbb{Q}(\alpha)$. By Theorem 3.3.1 and equation (3.1.2) we can suppose that α is a reciprocal algebraic integer. From Lemma 4.2.3, Lemma 2.3.1 and Lemma 3.1.2, we can suppose that $\mathrm{H}_{\mathbb{Q}(\alpha)} \neq \{\ 1\ \}$. From Lemma 4.2.2 and The Fundamental

Theorem of Galois Theory we can suppose that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ and consequently, by Lemma 4.3.3 that $\mathrm{H}_{\mathbb{Q}(\alpha)} \bigcap \langle\sigma\rangle = \{ 1 \}$.

By considering the distinct elements of G, it follows that there exists $i \in \{ 0, \ldots, 2m-1 \}$ such that $\mathrm{H}_{\mathbb{Q}(\alpha)} = \langle\sigma^i\tau\rangle$ and consequently that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2m$. By Lemma 4.3.2 we have that $\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\alpha)}) = \langle \mathrm{H}_{\mathbb{Q}(\alpha)}, \sigma^m \rangle$. As a result, $[\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\alpha)}) : \mathrm{H}_{\mathbb{Q}(\alpha)}] = 2$. It follows from The Fundamental Theorem of Galois Theory that $\sigma^m(\alpha) = 1/\alpha$ and that α and $1/\alpha$ are the only Galois conjugates of α contained in $\mathbb{Q}(\alpha)$.

We may suppose that α is extremal for the Mahler measure in $\mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. By Lemma 3.7.1, we can suppose that for all $s \in \mathbb{N}$ and all $g \in \mathrm{G} - \mathrm{H}_{\mathbb{Q}(\alpha)}$, $\alpha^s \neq g(\alpha)^s$. This will be useful as we will need to work with Lemma 2.5.6.

Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation wth respect to η. From Theorem 2.4.2 and Lemma 3.1.2 we assume that $\xi \notin \mathrm{Z_G}$. Let $i, j \in \{ 0, \ldots, 2m-1 \}$ such that $i \neq j$ and $i \neq j \pm m$. By Lemma 4.3.2,

$$\mathrm{N_G}(\langle\sigma^i\tau\rangle) \bigcap \mathrm{N_G}(\langle\sigma^j\tau\rangle) = \langle\sigma^m\rangle$$

Suppose that α_1, α_2, α_3, and α_4 are distinct Galois conjugates of α on the archimedean unit circle with respect to η. Then it follows that $\xi = \sigma^m \in \mathrm{Z_G}$ which would be a contradiction. It consequently follows that α can have at most two Galois conjugates on the archimedean unit circle. For our computations this will play a necessary role in estimates of the required specialization of the quantity $A \equiv \prod_{v \mid \infty} a_v^{(d_v/d)}$ contained in the hypothesis of Lemma 2.5.2.

4.5 Estimates for $\mathbf{A \equiv \prod_{v \mid \infty} a_v^{(d_v/d)}}$

We will need to work with Lemma 2.5.2 and in order to prove that $C_D = \mathrm{M}(x^3 - x - 1)$ we will need estimates for the quantity $A \equiv \prod_{v \mid \infty} a_v^{(d_v/d)}$ that are sharper than the trivial estimate obtained from the usual triangle inequality. Lemmas 4.5.1, 4.5.2, and 4.5.3 were developed for this purpose. In this section, let $|| \cdot ||_\infty$ be the usual archimedean absolute value on $\mathbb{C}$.

Lemma 4.5.1. *Let $z = re^{i\theta} \in \mathbb{C}$ such that $\theta \in \left[-\frac{\pi}{3}, \frac{\pi}{3}\right]$. Then*

$$\Big|\Big|z - 1\Big|\Big|_\infty \leq \max\Big\{\ 1,\ ||z||_\infty\ \Big\}$$

Proof. If $||z||_\infty \leq 1$ the lemma is trivial. Assume $||z||_\infty > 1$.

$$re^{i\theta} \ = \ r\cos\theta + ir\sin\theta$$

$Re\ z > 0.5$ and $||Re\ (z-1)||_\infty < ||Re\ z||_\infty$. $Im\ (z-1) = Im\ z$,

$$||z-1||_\infty^2 = (Re\ (z-1))^2 + (Im\ z)^2 \leq (Re\ z)^2 + (Im\ z)^2 = ||z||_\infty^2 \qquad \square$$

Lemma 4.5.2. *Let $z = re^{i\theta}$ such that $\theta \in \left[\frac{\pi}{2}, \frac{3\pi}{2}\right]$. Then*

$$\Big|\Big|z - 1\Big|\Big|_\infty \leq \Big(\ \sqrt{2}\ \Big) \cdot \Big(\ \sqrt{1 - \cos\theta}\ \Big) \cdot \max\Big\{\ 1,\ ||z||_\infty\ \Big\}$$

Proof. If $||z||_\infty \leq 1$, the lemma is trivial. Assume $||z||_\infty > 1$.

$$re^{i\theta} \;=\; r\cos\theta + ir\sin\theta$$

Let $a \;=\; \tan\theta$. Then

$$\cos\theta \;=\; \frac{-1}{\sqrt{a^2+1}}$$

Since

$$z \;=\; Re\ z + i(a\ Re\ z)$$

it follows that

$$||z||_\infty^2 \;=\; (a^2+1)(Re\ z)^2$$

and

$$||z-1||_\infty^2 = (1+a^2)(Re\ z)^2 - 2\ (Re\ z) + 1$$

The inequality

$$\Big|\Big|z-1\Big|\Big|_\infty \leq \Big(\ \sqrt{2}\ \Big)\cdot\Big(\ \sqrt{1-\cos\theta}\ \Big)\cdot\max\Big\{\ 1,\ ||z||_\infty\ \Big\}$$

is thus equivalent to

$$0 \;\leq\; (a^2+1)\big(2+\sqrt{a^2+1}\big)(Re\ z)^2 + 2\cdot\Big(\ \sqrt{a^2+1}\ \Big)\ (Re\ z) - \sqrt{a^2+1}$$

Let

$$A \;=\; \Big(\ a^2+1\ \Big)\Big(\ \sqrt{a^2+1}+2\ \Big)$$

$$B \;=\; 2\sqrt{a^2+1}$$

$$C \;=\; -\sqrt{a^2+1}$$

and

$$f(x) \;=\; Ax^2 + Bx + C$$

The last inequality is equivalent to $f(x) \;\geq\; 0$. We note that $f(0) < 0, \;\; f(1) \geq 0$ and

$$f\left(\frac{-1}{\sqrt{a^2+1}} \right) \;=\; 0$$

By The Intermediate Value Theorem and The Fundamental Theorem of Algebra it follows that for $Re\ z \leq -1/\sqrt{a^2+1} = \cos\theta$

$$||z-1||_\infty \;\leq\; \left(\sqrt{2 + \frac{2}{\sqrt{a^2+1}}} \right) \cdot \left(\;||z||_\infty \; \right)$$

$$||z-1||_\infty \;\leq\; \left(\sqrt{2} \right) \cdot \left(\sqrt{1-\cos\theta} \right) \cdot \left(\;||z||_\infty \; \right)$$

and since $||z||_\infty \geq 1$,

$$Re\ z \;\leq\; -\frac{1}{\sqrt{a^2+1}} \qquad \square$$

Lemma 4.5.3. *Let $z = re^{i\theta}$ such that $\theta \;\in\; \left[\frac{\pi}{3}, \frac{\pi}{2}\right] \bigcup \left[-\frac{\pi}{2}, -\frac{\pi}{3}\right]$. Then*

$$\Big|\Big|z-1\Big|\Big|_\infty \leq \left(\sqrt{2} \right) \cdot \left(\sqrt{1-\cos\theta} \right) \cdot \max\Big\{ \;1,\; ||z||_\infty \; \Big\}$$

Proof. If $||z||_\infty \leq 1$ the lemma is trivial. Assume $||z||_\infty \geq 1$. Let $a \;=\; \tan\theta$. Then

$$\cos\theta \;=\; \left(\frac{1}{\sqrt{a^2+1}} \right)$$

and

$$z \;=\; Re\ z + i(a\ Re\ z)$$

so that

$$||z||_\infty^2 \;=\; (a^2+1)(Re\ z)^2$$

and

$$||z-1||_\infty^2 \;=\; (a^2+1)(Re\ z)^2 - 2(Re\ z) + 1$$

The inequality,

$$\Big|\Big|z-1\Big|\Big|_\infty \leq \Big(\ \sqrt{2}\ \Big)\cdot\Big(\ \sqrt{1-\cos\theta}\ \Big)\cdot\max\Big\{\ 1,\ ||z||_\infty\ \Big\}$$

is equivalent to

$$0 \;\leq\; (\ a^2+1\ )(\ \sqrt{a^2+1}-2\ )(Re\ z)^2 + 2\cdot\sqrt{a^2+1}\ (Re\ z) - \sqrt{a^2+1}$$

Let

$$A \;=\; \Big(\ a^2+1\ \Big)\Big(\ \sqrt{a^2+1}-2\ \Big)$$

$$B \;=\; 2\sqrt{a^2+1}$$

$$C \;=\; -\sqrt{a^2+1}$$

and

$$f(x) \;=\; Ax^2 + Bx + C$$

The last inequality is equivalent to $f(x) \;\geq\; 0$

$$f\left(\ \frac{1}{\sqrt{a^2+1}}\ \right) \;=\; f(\cos\theta) \;=\; 0$$

Since $\theta \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right] \bigcup \left[-\frac{\pi}{2}, -\frac{\pi}{3}\right]$, we have $a^2 \geq 3$ and therefore $A \geq 0$. Since $B > 0$, if

$$Re\ z \geq \cos\theta \ = \ \frac{1}{\sqrt{a^2+1}}$$

then

$$f(Re\ z) \ \geq \ 0 \qquad \square$$

Lemmas 4.5.1, 4.5.2, and 4.5.3. each have symmetric versions where $z+1$ is considered as opposed to $z-1$. These symmetric versions have the same proofs as Lemmas 4.5.1, 4.5.2. and 4.5.3.

4.6 Numbers of Degree ≥ 10

Proposition 4.6.1. *Let $m \in \mathbb{N},\ m \geq 2$. Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \ \approx \ D_{2\cdot 2m}$. *Let $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. If 2 does not ramify in $\mathbb{K}$ then*

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{24} \right)$$

If 2 does not ramify in $\mathbb{K}$ and $f \leq 2$ then

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{6} \right)$$

Proof. Since $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ it follows that $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. Let

$\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle\sigma\rangle \rtimes_\rho \langle\tau\rangle$. Let $\mathcal{A}_2 \ = \ \{\ v_1,\ \ldots,\ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the 2−adic place of $\mathbb{Q}$. If $f \leq 2$, then

$$\alpha - \alpha^4 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 - \alpha^3 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

By the difference of squares formula,

$$1 - \alpha^6 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{6} \right)$$

If $f \geq 3$ then $\Phi_{v_1} \in \langle\sigma\rangle$ and $[\mathrm{G} : \mathrm{Z}_\mathrm{G}(\Phi_{v_1})] \leq 2$. By Theorem 1.9.1(i), G acts transitively by conjugation on the set of Frobenius automorphisms of the v_i. Consequently, we may suppose that

$$\Phi_{v_1} \ = \ \cdots \ = \ \Phi_{v_{t/2}}$$

As a result,

$$\Phi_{v_1}(\alpha) - \alpha^2 \ \in \ \mathcal{M}_{v_1} \cdots \mathcal{M}_{v_{t/2}}$$

By the difference of squares formula,

$$\Phi_{v_1}(\alpha^4) - \alpha^8 \ \in \ \mathcal{M}_{v_1}^3 \cdots \mathcal{M}_{v_{t/2}}^3$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{24} \right) \qquad \square$$

Proposition 4.6.2. *Let $m \in \mathbb{N}, \ m \geq 2$. Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \ \approx \ D_{2 \cdot 2m}$. *Let $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. If 2 ramifies in $\mathbb{K}$ and $e = 2$, then*

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{12} \right)$$

Proof. Since $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ it follows that $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle \sigma \rangle \rtimes_{\rho} \langle \tau \rangle$. Let $\mathcal{A}_2 \ = \ \{ \ v_1, \ \ldots, \ v_t \ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the 2−adic place of $\mathbb{Q}$. Suppose that $\exists \ i \ \in \ \{ \ 0, \ \ldots, \ 2m-1 \ \}$ such that $\mathrm{G}_0 = \langle \sigma^i \tau \rangle$. By Lemma 4.3.2 and Theorem

1.9.1, $f = 1$ or $f = 2$ and

$$\alpha - \alpha^4 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 - \alpha^3 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

By the difference of squares formula,

$$1 - \alpha^{12} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^4$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{12} \right)$$

If $e = 2$ and there does not exist $i \in \{ 0, \ldots, 2m-1 \}$ such that $\mathrm{G}_0 = \langle \sigma^i \tau \rangle$, then, by Lemma 4.3.1, $\mathrm{G}_0 = \mathrm{G}_1 = \langle \sigma^m \rangle$. By Theorem 1.9.1(i), G acts transitively by conjugation on the inertia groups of the v_i and by Lemma 4.3.4 $\sigma^m \in \mathrm{Z}_\mathrm{G}$. It follows that

$$\alpha - \sigma^m(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

By the difference of squares formula,

$$\alpha^2 - \sigma^m(\alpha^2) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_1}^4$$

By Lemma 3.7.1 and Section 4.4 we can assume that

$$0 \ \neq \ \alpha^2 - \sigma^m(\alpha^2)$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{4} \right) \quad \square$$

Proposition 4.6.3. *Let* $m \in \mathbb{N}$, $m \geq 5$. *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx D_{2\cdot 2m}$. *Let* $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$ *be such that* $\mathbb{K}$ *is the Galois closure of* $\mathbb{Q}(\alpha)$. *If* 2 *ramifies with ramification index greater than* 2, *then* $\mathrm{M}(x^3 - x - 1) \leq \mathrm{M}(\alpha)$.

Proof. Since $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ it follows that $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle \sigma \rangle \rtimes_{\rho} \langle \tau \rangle$. By Theorem 3.3.1, we suppose that α is reciprocal. Recall the allowed assumptions on α and $\mathrm{H}_{\mathbb{Q}(\alpha)}$ from Section 4.4. Let $\mathcal{A}_2 \ = \ \{\ v_1, \ \ldots \ , \ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the 2-adic place of $\mathbb{Q}$. We will use Theorem 1.9.1 and Lemma 3.1.2 throughout the proof.

CASE 1: $e \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]/4$. By considering the distinct elements of G, there

exists $i \in \{ 1, \ldots, 2m-1 \}$ such that $\sigma^i \in \mathrm{G}_0$. Let $s \in \mathbb{N}$ be minimal such that $2^s > e$. Then $2^s < 4e \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$. As a result, $2^{s+1} \leq 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$. By Lemma 2.5.6 with $m \geq 0$ and $n = 1$,

$$h(\alpha) \geq \left(\frac{\log 2}{2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \right)$$

and by Lemma 3.1.2,

$$\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$$

CASE 2: $3e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even, it follows that $2 \mid e$. Suppose that $\sigma^m \in \mathrm{G}_{v_1,1}$. Let $r \in \mathbb{N}$ be smallest such that $2^r \geq e$. Then $2^{r+1} < 4e = (4/3) \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Since $\sigma^m(\alpha) = 1/\alpha$ and α is a unit

$$\alpha - \sigma^m(\alpha) \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

$$\alpha - \frac{1}{\alpha} \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

$$\alpha^2 - 1 \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

By the difference of squares formula,

$$\alpha^{2^{r+1}} - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

By Lemmas 2.5.1, 2.5.2, and since

$$2^{r+1} \ < \ \left(\ \frac{4 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]}{3} \ \right)$$

we have

$$h(\alpha) \ \geq \ \left(\ \frac{3 \cdot \log 2}{4 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \ \right)$$

it follows from Lemma 3.1.2 that

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

Suppose now that $\sigma^m \notin \mathrm{G}_{v_1,0}$. Then, by Lemma 4.3.10, $e = 6$ and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 18$. Since $e = 6$ there exists $j \ \in \ \{ \ 1, \ \ldots \ , \ 2m - 1 \ \}$ such that $\sigma^j \ \in \ \mathrm{G}_{v_1,0}$. From Lemma 3.7.1 and the difference of squares formula we deduce that

$$\alpha - \sigma^j(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

$$0 \neq \alpha^{16} - \sigma^j(\alpha^{16}) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

By Lemma 2.5.1 and Lemma 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{32} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

CASE 3: $2e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Let $r \in \mathbb{N}$ be minimal such that $2^r \geq e$. Then $2^{r+1} < 4e \ = \ 2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. If $\sigma^m \ \in \ \mathrm{G}_{v_1,1}$, then since $\sigma^m(\alpha) = 1/\alpha$, α is a unit and the difference of squares formula

$$\alpha - \sigma^m(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

$$\alpha - \frac{1}{\alpha} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

$$\alpha^2 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

$$\alpha^{2^{r+1}} - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^{2e}$$

By Lemmas 2.5.1 and 2.5.2 and since $2^{r+1} < 2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$, we have

$$h(\alpha) \ \geq \ \left(\ \frac{\log 2}{2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \ \right)$$

and by Lemma 3.1.2 that

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

From Lemma 4.3.10 we are left with the case $e = 6$ or equivalently $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 12$. In this case $\sigma^4 \in \mathrm{G}_{v_1,0}$ and by Lemma 3.7.1 and the difference of squares formula

$$\alpha - \sigma^4(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v$$

$$0 \neq \alpha^{16} - \sigma^4(\alpha^{16}) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^{14}$$

By Lemmas 2.5.1 and 2.5.2, we have

$$h(\alpha) \ \geq \ \left(\ \frac{\log 2}{24} \ \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

CASE 4: $e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then $f = 1$ or $f = 2$. Let $r \in \mathbb{N}$ be minimal such that $2^r \geq 2e$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even and ≥ 10, if $f = 1$, then G is a 2 group, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 16$, and

$$\alpha - \alpha^2 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

$$\alpha \cdot (1 - \alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 - \alpha \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

By the difference of squares formula,

$$1 - \alpha^{2[\mathbb{Q}(\alpha):\mathbb{Q}]} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $f = 2$, then the only odd prime power possibly dividing e is 3 and $\mathcal{A}_2 = \{ v_1 \}$. If $f = 2$ and $3 \nmid e$ then G is a 2 group, $e \geq 16$, $\sigma^m \in \mathrm{G}_{v_1,3}$, and

$$\alpha - \sigma^m(\alpha) \ \in \ \mathcal{M}_{v_1}^4$$

Since $\sigma^m(\alpha) = \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \mathcal{M}_{v_1}^4$$

Since α is an integer,

$$\alpha^2 - 1 \ \in \ \mathcal{M}_{v_1}^4$$

By the difference of squares formula,

$$1 - \alpha^{[\mathbb{Q}(\alpha):\mathbb{Q}]} \ \in \ \mathcal{M}_{v_1}^{2e}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $f = 2$ and $3 \mid e$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 12$ and there exists $s \in \mathbb{N}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s \cdot 3$. In this case, $\sigma^m \in G_{v_1,1}$ so that

$$\alpha - \sigma^m(\alpha) \ \in \ \mathcal{M}_{v_1}^2$$

Since $\sigma^m(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \mathcal{M}_{v_1}^2$$

Since α is an integer,

$$\alpha^2 - 1 \ \in \ \mathcal{M}_{v_1}^2$$

Suppose $e = 12$. By the difference of squares formula,

$$\alpha^{32} - 1 \ \in \ \mathcal{M}_{v_1}^{28}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{24} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e \geq 24$, then $\sigma^m \in G_{v_1,2}$ and

$$\alpha - \sigma^m(\alpha) \ \in \ \mathcal{M}_{v_1}^{3}$$

Since $\sigma^m(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \mathcal{M}_{v_1}^{3}$$

Since α is an integer,

$$\alpha^2 - 1 \ \in \ \mathcal{M}_{v_1}^{3}$$

$$(\alpha - 1)(\alpha + 1) \ \in \ \mathcal{M}_{v_1}^3$$

Since $\mathcal{M}_{v_1}$ is a prime ideal of $\mathcal{O}_{v_1}$,

$$\alpha - 1 \ \in \ \mathcal{M}_{v_1}^2$$

By the difference of squares formula,

$$\alpha^{2^{s+1}} - 1 \ \in \ \mathcal{M}_{v_1}^{2^{s+2}}$$

$$\alpha^{2^{s+2}} - 1 \ \in \ \mathcal{M}_{v_1}^{2e}$$

Since

$$2^{s+2} \ = \ \left(\ \frac{4 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]}{3} \ \right)$$

it follows from Lemmas 2.5.1 and 2.5.2 that

$$h(\alpha) \ \geq \ \left(\ \frac{3 \cdot \log 2}{4 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \ \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

CASE 5: $e = 2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then $f = 1$, G is a 2 group, $\mathcal{A}_2 = \{ \ v_1 \ \}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 16$. Consequently, $\sigma^m \in \mathrm{G}_{v_1,3}$ and

$$\alpha - \sigma^m(\alpha) \ \in \mathcal{M}_{v_1}^4$$

Since $\sigma^m(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \mathcal{M}_{v_1}^4$$

Since α is an integer,

$$\alpha^2 - 1 \ \in \ \mathcal{M}_{v_1}^4$$

By the difference of squares formula,

$$\alpha^{2[\mathbb{Q}(\alpha):\mathbb{Q}]} - 1 \ \in \ \mathcal{M}_{v_1}^{2e}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \geq \left(\frac{\log 2}{2 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

CASE 6: $e \ \in \ \{ \ (2/3) \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}], \ (2/5) \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}], \ (2/7) \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \ \}$

Then $\sigma^m \ \in \ \mathrm{G}_{v_1,1}$ and

$$\alpha - \sigma^m(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

Since $\sigma^m(\alpha) \ = \ \alpha$

$$\alpha - \frac{1}{\alpha} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

Since α is an integer

$$\alpha^2 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

By the difference of squares formula

$$(\alpha + 1)(\alpha - 1) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

Since the $\mathcal{M}_v$ are prime ideals

$$\alpha - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v$$

Since $\mathrm{H}_{\mathbb{Q}(\alpha)} \leq \mathrm{G}_0$

$$\alpha - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^2$$

Let $s \ \in \ \mathbb{N}$ be minimal such that $2^s > \dfrac{2}{3}[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq e$. Then

$$2^s \ < \ \frac{4}{3}[\mathbb{Q}(\alpha) : \mathbb{Q}]$$

and by the difference of squares formula

$$\alpha^{2^s} - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_v^{2e}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{3 \cdot \log 2}{4 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1) \qquad \square$$

4.7 Numbers of Degree ≤ 8

Proposition 4.7.1. ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$). *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx D_{2\cdot 4}$. *Let* $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$. *be such that* $\mathbb{K}$ *is the Galois closure of* $\mathbb{Q}(\alpha)$. *Then* $\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$.

Proof. Since $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ it follows that $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle\sigma\rangle \rtimes_{\rho} \langle\tau\rangle$. By Theorem 3.3.1, we suppose that α is reciprocal. Let $\mathcal{A}_2 = \{\ v_1,\ \ldots,\ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the 2−adic place of $\mathbb{Q}$. Let $\eta :\ \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding of $\mathbb{K}$ into $\mathbb{C}$ and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. By Theorem 3.6.1, we suppose that $\xi \notin \mathrm{Z_G}$. Suppose that α does not have a real Galois conjugate. By Theorem 2.2.1, we can assume that α has a Galois conjugate γ such that $\beta = \gamma \cdot \xi(\gamma) > 1$. Recall the allowed assumptions on $\mathrm{H}_{\mathbb{Q}(\alpha)}$ established in Section 4.4. Since $\sigma^2(\beta) = 1/\beta$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$, we can deduce that $\mathrm{M}(\alpha) = \mathrm{M}(\beta)$. It follows that we may assume α to be real and positive. In this case, $\mathrm{M}(\alpha) = \alpha$.

CASE 1: 2 does not ramify in $\mathbb{K}$. By Proposition 4.6.1, we assume that $f = 4$ and consequently that $\mathcal{A}_2 = \{\ v_1,\ v_2\ \}$ and $\Phi_{v_1}^2 = \Phi_{v_2}^2 = \sigma^2$. As a result,

$$\sigma^2(\alpha) - \alpha^4 \ \in \ \mathcal{M}_{v_1} \bigcap \mathcal{M}_{v_2}$$

Since $\sigma^2(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\frac{1}{\alpha} - \alpha^4 \ \in \ \mathcal{M}_{v_1} \bigcap \mathcal{M}_{v_2}$$

Since α is an integer,

$$1 - \alpha^5 \ \in \ \mathcal{M}_{v_1} \bigcap \mathcal{M}_{v_2}$$

By the difference of squares formula,

$$1 - \alpha^{10} \ \in \ \mathcal{M}_{v_1}^2 \bigcap \mathcal{M}_{v_2}^2$$

Let $\delta \equiv 1 - \alpha^{10}$ and for each $v \mid \infty$, define $a_v \ \in \ \mathbb{R}^+$ by

$$a_v \ \equiv \ \frac{\left|\left|\ \delta\ \right|\right|_v}{\max\left\{\ 1,\ ||\alpha^{10}||_v\ \right\}}$$

Let

$$A \equiv \prod_{v \ \mid \ \infty} a_v^{(d_v/d)}$$

By Lemma 4.5.1, since $\alpha \in \mathbb{R}^+$, $A \leq \sqrt{2}$. By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \geq \left(\frac{1}{10} \right) \left(\log \frac{4}{\sqrt{2}} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$$

CASE 2: 2 ramifies in $\mathbb{K}$. If $e = 2$ and $\sigma^2 \in \mathrm{G}_{v_1,1}$ then

$$\alpha - \sigma^2(\alpha) \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^e$$

Since $\sigma^2(\alpha) = \frac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^e$$

Since α is an integer,

$$\alpha^2 - 1 \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^e$$

By the difference of squares formula,

$$\alpha^4 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{4} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e = 2$ and $\exists \ i \ \in \ \{ \ 0, \ 1, \ 2, \ 3 \ \}$ such that $\mathrm{G}_0 \ = \ \langle \sigma^i \tau \rangle$ then by Lemma 4.3.2 and Theorem 1.9.1 $f \leq 2$. As a result,

$$\alpha^4 - \alpha \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since α is a unit,

$$\alpha^3 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

By the difference of squares formula,

$$\alpha^{12} - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

Let $\delta \equiv \alpha^{12} - 1$ and for each archimedean place v, let a_v be defined as

$$a_v \ \equiv \ \frac{|| \ \delta \ ||_v}{\max\Big\{ \ 1, \ ||\alpha||^{12} \ \Big\}}$$

Define

$$A \ \equiv \ \prod_{v \ | \ \infty} {a_v}^{(d_v/d)}$$

By Lemma 4.5.1, $A \leq \sqrt{2}$. By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\ \frac{1}{12} \ \right) \left(\ \log \frac{4}{\sqrt{2}} \ \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e = 4$, then $\sigma^2 \in \mathrm{G}_{v_1,1}$ and

$$\alpha - \sigma^2(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2}$$

Since $\sigma^2(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

Since α is a unit,

$$\alpha^2 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

By the difference of squares formula,

$$\alpha^8 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{8} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e = 8$, then $\mathcal{A}_2 = \{ \ v_1 \ \}, \ \sigma^2 \in \mathrm{G}_{v_1,2}$ and

$$\alpha - \sigma^2(\alpha) \ \in \ \mathcal{M}_{v_1}^3$$

Since $\sigma^2(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \mathcal{M}_{v_1}^3$$

Since α is a unit,

$$\alpha^2 - 1 \ \in \ \mathcal{M}_{v_1}^3$$

By the difference of squares formula

$$(\alpha + 1)(\alpha - 1) \in \mathcal{M}_{v_1}^3$$

Since $\mathcal{M}_{v_1}$ is a prime ideal of $\mathcal{O}_{v_1}$,

$$\alpha - 1 \ \in \ \mathcal{M}_{v_1}^2$$

By the difference of squares formula,

$$\alpha^8 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_1}^{2e}$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{8} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1) \qquad \square$$

Proposition 4.7.2. ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$) *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \ \approx \ D_{2 \cdot 6}$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$ *be such that* $\mathbb{K}$ *is the Galois closure of* $\mathbb{Q}(\alpha)$. *Then* $\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$.

Proof. Since $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ it follows that $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle \sigma \rangle \rtimes_{\rho} \langle \tau \rangle$. By Theorem 3.3.1, we suppose that α is reciprocal. Let $\mathcal{A}_2 \ = \ \{\ v_1, \ \ldots \ , \ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the $2-$adic place of $\mathbb{Q}$. Let $\eta : \ \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. By Theorem 3.6.1, we can assume that $\xi \notin \mathrm{Z}_{\mathrm{G}}$. Recall the allowed assumptions on $\mathrm{H}_{\mathbb{Q}(\alpha)}$ established in Section 4.4.

CASE 1: 2 ramifies in $\mathbb{K}$. By Proposition 4.6.2 and Lemma 3.1.2, we assume $e \geq 3$. If $e = 4$, then $\sigma^3 \in \mathrm{G}_{v_1,1}$ and,

$$\alpha - \sigma^3(\alpha) \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_1}^2$$

Since $\sigma^3(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_1}^2$$

Since α is a unit,

$$\alpha^2 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

By the difference of squares formula,

$$\alpha^8 - 1 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^{2e}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{8} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e = 3$, then $\sigma^2 \in \mathrm{G}_{v_1,0}$ and

$$\sigma^2(\alpha) - \alpha \ \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

By the difference of squares formula and Lemma 3.7.1,

$$0 \neq \sigma^2(\alpha^8) - \alpha^8 \ \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^7$$

By Lemmas 2.5.1 and 2.5.2,

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{12} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e = 6$ then $f = 2$ and $\mathcal{A}_2 \ = \ \{ \ v_1 \ \}$. If $\sigma^3 \in \mathrm{G}_{v_1,1}$,

$$\alpha - \sigma^3(\alpha) \ \in \ \mathcal{M}_{v_1}^2$$

Since $\sigma^3(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\alpha - \frac{1}{\alpha} \ \in \ \mathcal{M}_{v_1}^2$$

Since α is an integer,

$$\alpha^2 - 1 \ \in \ \mathcal{M}_{v_1}^2$$

By the difference of squares formula,

$$\alpha^{16} - 1 \ \in \ \mathcal{M}_{v_1}^{14}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{12} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $e = 6$ and $\sigma^3 \notin \mathrm{G}_{v_1,1}$, then $\mathrm{G}_{v_1,0} \approx D_{2\cdot 3}$. We can assume that $\tau \in \mathrm{G}_{v_1,1}$ and that $\tau \ \notin \ \mathrm{H}_{\mathbb{Q}(\alpha)}$. Thus,

$$0 \ \neq \ \alpha - \tau(\alpha) \in \mathcal{M}_{v_1}^2$$

By the difference of squares formula and Lemma 3.7.1,

$$0 \neq \alpha^8 - \tau(\alpha^8) \in \mathcal{M}_{v_1}^{14}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \geq \left(\frac{\log 2}{12} \right)$$

By Lemma 3.1.2

$$\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$$

CASE 2: 2 does not ramify in $\mathbb{K}$.

By Proposition 4.6.1, we assume that $f \geq 3$. If $f = 3$ then

$$\alpha - \alpha^8 \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 \pm \alpha^7 \in \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

By the difference of squares formula,

$$1 - \alpha^{14} \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}^2$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{\log 2}{14} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ \geq \ \mathrm{M}(x^3 - x - 1)$$

If $f = 6$, then $\mathcal{A}_2 \ = \ \{ \ v_1, \ v_2 \ \}$ and $\Phi_{v_1}^3 = \Phi_{v_2}^3 = \sigma^3$ so that

$$\Phi_{v_1}^3(\alpha) - \alpha^8 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since $\sigma^3(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\frac{1}{\alpha} - \alpha^8 \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 \pm \alpha^9 \ \in \ \bigcap_{\mathcal{A}_2} \mathcal{M}_{v_i}$$

Assume that α is not real and is outside the closed archimedean unit disk with respect to η. Since α is reciprocal of degree 6, α has either two Galois conjugates on the archimedean unit circle or α has two Galois conjugates that are real and none on the archimedean unit circle with repecct to η.

CASE 2(a): No Real Galois Conjugates. Suppose that α has no real Galois conjugates. Let $\gamma \equiv \alpha^9$. By Lemma 3.7.1, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. By considering $-\gamma, -\overline{\gamma}$, and $\overline{\gamma}$ if necessary, assume that γ is in the first quadrant. By The Fundamental Theorem of Galois Theory, there exists a subfield, $\mathbb{F}$, of $\mathbb{Q}(\gamma)$ that is quadratic over $\mathbb{Q}$. Let $\mathrm{H}_{\mathbb{F}}$ be the subgroup of G that fixes the field $\mathbb{F}$. Let $g_1,\ g_2,\ g_3$ be a complete set of distinct coset representatives of $\mathrm{H}_{\mathbb{Q}(\gamma)}$ in $\mathrm{H}_{\mathbb{F}}$. Since $h(g_1(\alpha)g_2(\alpha)g_3(\alpha)) \leq 3 \cdot h(\alpha),\ \ 3 \cdot [\mathbb{Q}(g_1(\alpha)g_2(\alpha)g_3(\alpha)) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$, 2 does not ramify in $\mathbb{K}$, Lemma 4.3.5 and $g_1(\alpha)g_2(\alpha)g_3(\alpha)$ is an abelian integer of degree less than or equal to 2, we assume that $g_1(\gamma)g_2(\gamma)g_3(\gamma) = \big((g_1(\alpha)g_2(\alpha)g_3(\alpha)\big)^9 = \pm 1$. It then follows that one of $\gamma_u \equiv \pm\gamma/\overline{\gamma}$ is a Galois conjugate of γ on the archimedean unit circle.

Case (2a1): $\gamma_{\mathbf{u}} \equiv +\gamma/\overline{\gamma}$

It follows that the arguement of either γ_u or $\overline{\gamma}_u$ is twice that of γ. Let $\delta_1 \equiv \gamma - 1$. For each place $v \mid \infty$, let

$$a_{v_1} \equiv \frac{|| \delta_1 ||_v}{\max\left\{ 1, ||\gamma||_v \right\}}$$

Let

$$A_1 = \prod_{v \mid \infty} a_{v_1}^{(d_v/d)}$$

If γ is in the sector $\Big[0, 17.75\pi/48\Big]$, then, by Lemmas 4.5.1 and 4.5.2,

$$A_1 \leq \sqrt[6]{2 - 2\cos(35.5\pi/48)} \cdot \sqrt[3]{2 - 2\cos(17.75\pi/48)}$$

$$= 1.30261$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \geq \left(\frac{1}{9} \right) \cdot \left(\log \frac{2}{A_1} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \geq 1.331 \geq \mathrm{M}(x^3 - x - 1)$$

Let $\delta_2 \equiv \gamma + 1$. For each place $v \mid \infty$, let

$$a_{v_2} \equiv \frac{|| \delta_2 ||_v}{\max\left\{ 1, ||\gamma||_v \right\}}$$

Let

$$A_2 \equiv \prod_{v \mid \infty} a_{v_2}^{(d_v/d)}$$

If γ is in the sector $\left[17.75\pi/48, \pi/2\right]$ then, by the symmetric version of Lemma 4.5.2 and since γ_u is on the archimedean unit circle with respect to η,

$$A_2 \leq \sqrt[6]{2 + 2\cos(35.5\pi/48)} \cdot \sqrt[3]{2 + 2\cos(17.75\pi/48)}$$

$$= 1.30257$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \geq \left(\frac{1}{9} \right) \cdot \left(\log \frac{2}{A_2} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \geq 1.329 \geq \mathrm{M}(x^3 - x - 1)$$

This completes the proof of the case 2(a1).

Case (2a2): $\gamma_{\mathbf{u}} \equiv -\gamma/\overline{\gamma}$

It follows that either the arguement of γ_u or the arguement of $\overline{\gamma}_u$ is π + twice the arguement of γ. Let $\delta_1 \equiv \gamma - 1$. For each place $v \mid \infty$, let

$$a_{v_1} \equiv \frac{|| \delta_1 ||_v}{\max\left\{ 1, ||\gamma||_v \right\}}$$

Let

$$A_1 \equiv \prod_{v \mid \infty} a_{v_1}^{(d_v/d)}$$

Then, by Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \geq \left(\frac{1}{9} \right) \left(\log \frac{2}{A_1} \right)$$

If γ is in the sector $\left[0, \pi/3\right]$, then, by Lemmas 4.5.1 and 4.5.2, $A_1 \leq 2^{1/3}$ so that $\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$. If γ is in the sector $\left[\pi/3, \pi/2\right]$ then γ_u is in the sector $\left[-\pi/3, 0\right]$ so that $A_1 \leq 2^{1/3}$ and $\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$. This completes the proof of case 2(a2).

CASE 2(b): Real Galois Conjugates. Suppose now that $\gamma \equiv \alpha^9$ has a real Galois conjugate, β. We can assume that $||\beta||_\infty \leq 1.33^{9/2}$. Let γ_3 be a Ga-

lois conjugate of γ that is not real. By considering $-\gamma_3, -\overline{\gamma_3}$, and $\overline{\gamma}_3$, if necessary, we can assume that γ_3 is in the first quadrant. Let $\delta \equiv \gamma - 1$. For each place $v \mid \infty$, let

$$a_v \;\equiv\; \frac{\left|\left|\; \delta \;\right|\right|_v}{\max\left\{\; 1,\; ||\gamma||_v \;\right\}}$$

Let

$$A \;\equiv\; \prod_{v \;\mid\; \infty} a_v^{(d_v/d)}$$

Suppose γ_3 is in the sector $\Big[0,\; \pi/3\Big]$. By Lemma 4.5.1,

$$A \;\leq\; 2^{1/3}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \;\geq\; \left(\; \frac{1}{9} \;\right) \cdot \left(\; \log \frac{2}{A} \;\right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \;\geq\; \mathrm{M}(x^3 - x - 1)$$

Suppose $\beta < 0$ and that γ_3 is in the sector $\Big[\pi/3,\; \pi/2\Big]$. Let $\delta \equiv \gamma + 1$. For each place $v \mid \infty$, let

$$a_v \;\equiv\; \frac{\big|\big|\ \delta\ \big|\big|_v}{\max\Big\{\ 1,\ ||\gamma||_v\ \Big\}}$$

Let

$$A \;=\; \prod_{v\ |\ \infty} a_v^{(d_v/d)}$$

By the symmetric version of Lemma 4.5.1,

$$A \;\leq\; 3^{1/3} \cdot \left(1 + \frac{1}{\beta}\right)^{1/3}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \;\geq\; \left(\ \frac{1}{9}\ \right) \cdot \left(\ \log \frac{2}{A}\ \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \;\geq\; \mathrm{M}(x^3 - x - 1)$$

Suppose $\beta > 0$ and γ_3 is in the sector $\Big[\pi/3,\ \pi/2\Big]$. Let $\delta \equiv \gamma - 1$. For each place $v \mid \infty$, let

$$a_v \;\equiv\; \frac{\big|\big|\ \delta\ \big|\big|_v}{\max\Big\{\ 1,\ ||\gamma||_v\ \Big\}}$$

Let

$$A \;\equiv\; \prod_{v\ |\ \infty} a_v^{(d_v/d)}$$

Then, by Lemmas 4.5.1 and 4.5.2,

$$A \;\leq\; 3^{1/3} \cdot \left(1 - \frac{1}{\beta}\right)^{1/3}$$

By Lemmas 2.5.1 and 2.5.

$$h(\alpha) \;\geq\; \left(\ \frac{1}{9}\ \right) \cdot \left(\ \log \frac{2}{A}\ \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \;\geq\; \mathrm{M}(x^3 - x - 1) \qquad \square$$

Proposition 4.7.3. **(** $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ **)** *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension such that* $\mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) \approx D_{2\cdot 8}$. *Let* $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$ *be such that* $\mathbb{K}$ *is the Galois closure of* $\mathbb{Q}(\alpha)$. *Then* $\mathrm{M}(\alpha) \geq \mathrm{M}(x^3 - x - 1)$.

Proof. Since $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$ it follows that $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. Let $\mathrm{G} \equiv \mathrm{Aut}(\ \mathbb{K}/\mathbb{Q}\ ) = \langle\sigma\rangle \rtimes_{\rho} \langle\tau\rangle$. By Theorem 3.3.1, we suppose that α is reciprocal. Let $\eta :\ \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation. By Theorem 3.6.1, we can assume that $\xi \notin \mathrm{Z}_{\mathrm{G}}$. Recall the allowed assumptions on $\mathrm{H}_{\mathbb{Q}(\alpha)}$ established in Section 4.4. Let $\mathcal{A}_3 = \{\ v_1,\ \ldots,\ v_t\ \}$ (where $t \in \mathbb{N}$) be the set of places of $\mathbb{K}$ that restrict to the 3−adic place of $\mathbb{Q}$.

Suppose that 3 does not ramify in $\mathbb{K}$. If $f \leq 2$ then

$$\alpha - \alpha^9 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 - \alpha^8 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

It then follows from Lemmas 2.5.1 and 2.5.2 that

$$h(\alpha) \ \geq \ \left(\ \frac{1}{8}\ \right) \cdot \left(\ \log \frac{3}{2}\ \right)$$

By Lemma 3.1.2

$$\mathrm{M}(\alpha) \ > \ \mathrm{M}(x^3 - x - 1)$$

If $f \ \geq \ 3$ then from Section 4.3 and Theorem 1.9.1, $[\mathrm{G} : \mathrm{Z}_{\mathrm{G}}(\Phi_{v_1})] = 2$

and

$$\Phi_{v_1}(\alpha) - \alpha^3 \ \in \ \bigcap_{i=1}^{t/2} \mathcal{M}_{v_i}$$

From the binomial theorem

$$\Phi_{v_1}(\alpha)^3 - \alpha^9 \ \in \ \bigcap_{i=1}^{t/2} \mathcal{M}_{v_i}^2$$

Let $\gamma \equiv \Phi_{v_1}(\alpha)^3/\alpha^9$ and $d = [\mathbb{Q}(\gamma) : \mathbb{Q}]$. Since α is a unit,

$$\gamma - 1 \ \in \ \bigcap_{i=1}^{t/2} \mathcal{M}_{v_i}^2$$

Since

$$\gamma + 1 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{O}_{v_i}$$

it follows from the difference of squares formula that

$$\gamma^2 - 1 \ \in \ \bigcap_{i=1}^{t/2} \mathcal{M}_{v_i}^2$$

For each archimedean place v of $\mathbb{K}$ let

$$a_v \equiv \frac{\left|\left|\gamma - 1\right|\right|_v}{\max\left\{ 1, ||\gamma||_v \right\}}$$

and

$$c_v \equiv \frac{\left|\left|\gamma^2 - 1\right|\right|_v}{\max\left\{ 1, ||\gamma^2||_v \right\}}$$

Let

$$A_1 \equiv \prod_{v \mid \infty} {a_v}^{(d_v/d)}$$

and

$$A_2 \equiv \prod_{v \mid \infty} {c_v}^{(d_v/d)}$$

By Lemmas 2.5.1 and 2.5.2 we have

$$h(\alpha) \geq \left(\frac{1}{12} \right) \cdot \left(\log \frac{3}{A_1} \right) \tag{4.7.1}$$

and

$$h(\alpha) \geq \left(\frac{1}{24} \right) \cdot \left(\log \frac{3}{A_2} \right) \tag{4.7.2}$$

If $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 16$ then, since $\xi \notin \mathrm{Z_G}$, $\mathbb{K} = \mathbb{Q}(\gamma)$, $\mathbb{K}$ is not totally real and $\sigma^4(\gamma) = 1/\gamma$, the Galois conjugates of γ occur in sets of four as $\gamma,\ \overline{\gamma},\ 1/\gamma,\ 1/\overline{\gamma}$. Suppose that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 8$ and that γ does not have a real Galois conjugate. Then the Galois conjugates occur in sets of four as $\gamma,\ \overline{\gamma},\ 1/\gamma,\ 1/\overline{\gamma}$.

Consequently either $1/2$ the conjugates of γ lie in the sector $\left[-5\pi/6,\ 5\pi/6\right]$ or $3/4$ the conjugates of γ^2 lie in the sector $\left[-\pi/3,\ \pi/3\right]$. If γ has a real conjugate then $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 8$. By Lemmas 4.5.1, 4.5.2 and 4.5.3 we have that either

$$A_1 \ \leq \ \sqrt{2} \cdot \sqrt[4]{2 + \sqrt{3}}$$

or

$$A_2 \ \leq \ \sqrt[4]{2}$$

It then follows from inequalities (4.7.1) and (4.7.2) that

$$\mathrm{M}(\alpha) \ > \ \mathrm{M}(x^3 - x - 1)$$

Suppose that 3 ramifies in $\mathbb{K}$. By Theorem 1.9.1 and Lemma 4.3.8 we know that $ef \leq 8$. If $f = 1$ then, by Theorem 1.9.1, $e = 2$ and

$$\alpha - \alpha^3 \ \in \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

Since α is a unit,

$$1 - \alpha^2 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

By the binomial theorem

$$1 - \alpha^6 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}^e$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{1}{6} \right) \cdot \left(\log \frac{3}{2} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ > \ \mathrm{M}(x^3 - x - 1)$$

We thus suppose that $f \geq 2$ and $e \leq 4$. If there exists $j \in \{ \ 2, \ 4 \ \}$ such that $\sigma^j \ \in \ \mathrm{G}_{v_1,0}$ then,

$$\sigma^j(\alpha) - \alpha \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

From the binomial theorem and Lemma 3.7.1,

$$0 \neq \sigma^j(\alpha)^3 - \alpha^3 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}^{\min\{e,3\}}$$

If $e = 2$ it follows from Lemmas 2.5.1 and 2.5.2 that

$$h(\alpha) \ \geq \ \left(\frac{1}{6} \right) \cdot \left(\log \frac{3}{2} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ > \ \mathrm{M}(x^3 - x - 1)$$

If $e = 4$ then by the binomial theorem and Lemma 3.7.1,

$$0 \ \neq \ \sigma^j(\alpha)^9 - \alpha^9 \ \in \ \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}^{7}$$

By Lemmas 2.5.1 and 2.5.2

$$h(\alpha) \ \geq \ \left(\frac{1}{18} \right) \cdot \left(\log \frac{3^{7/4}}{2} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ > \ \mathrm{M}(x^3 - x - 1)$$

We consequently assume that there exists $i \ \in \ \{ \ 0, \ 1, \ 2, \ 3, \ 4, \ 5, \ 6, \ 7 \ \}$

such that $\mathrm{G}_{v_1,0} = \langle \sigma^i \tau \rangle$ and that σ^4 acts as Φ_{v_1} it consequently follows that

$$\sigma^4(\alpha) - \alpha^3 \ \in \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

Since $\sigma^4(\alpha) \ = \ \dfrac{1}{\alpha}$

$$\frac{1}{\alpha} - \alpha^3 \ \in \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

Since α is a unit

$$1 - \alpha^4 \ \in \bigcap_{\mathcal{A}_3} \mathcal{M}_{v_i}$$

From the binomial theorem

$$1 - \alpha^{12} \ \in \bigcap_{\mathcal{A}_3} \mathcal{M}^3_{v_i}$$

From Lemmas 2.5.1 and 2.5.2 it follows that

$$h(\alpha) \ \geq \ \left(\frac{1}{12} \right) \cdot \left(\log \frac{3 \cdot \sqrt{3}}{2} \right)$$

and by Lemma 3.1.2

$$\mathrm{M}(\alpha) \ > \ \mathrm{M}(x^3 - x - 1) \qquad \square$$

We have thus proved the following

Theorem 4.7.4. (Garza) *Amongst all polynomials in $\mathbb{Z}[x]$ whose splitting fields are contained in dihedral Galois extensions of $\mathbb{Q}$, the lowest Mahler measure (other than 1) is attained by $x^3 - x - 1$.*

4.8 Final Remarks

We note that we have not established a lower bound for the height in dihedral extensions of the rationals. We hence state the following research question.

Research Problem 4. Establish a lower bound for the height in dihedral extensions of the rationals or exhibit a sequence of algebraic numbers, different from zero and the roots of unity and lying in dihedral extensions of the rationals, whose heights approach 0.

In both the archimedean and non-archimedean cases, we have established connections between the normalizer of a stabilizer and lower bounds for the height. Corollary 2.6.2 showed that lower bounds for the height exist in certain non-abelian isomorphism classes of Galois extensions. We propose the following research questions.

Research Problem 5. Establish a lower bound for the Mahler measure of

elements of $\overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$ whose Galios closures are Kummer extensions of cyclotomic extensions of the rationals.

Research Problem 6. Establish a lower bound for the Mahler measure of elements of $\overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$ whose Galios closures are meta-abelian extensions of the rationals.

Research Problem 7. Establish a lower bound for the Mahler measure of elements of $\overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$ whose Galios closures are $2-$group extensions of the rationals.

Research Problem 8. Establish a lower bound for the Mahler measure of elements of $\overline{\mathbb{Q}}^{\times} - \mathrm{Tor}(\ \overline{\mathbb{Q}}^{\times}\ )$ whose Galois closures are solvable extensions of the rationals.

Bibliography

[Am00a] F. Amoroso and R. Dvornicich. *A lower bound for the height in abelian extensions.* J. Number Theory **80** (2000), 260-272.

[Am00b] F. Amoroso and U. Zannier. *A relative Dobrowolski Lower Bound over Abelian Extensions.* Ann. Scoula Norm Sup. Pisa Cl. Sci. (4) Vol XXIX (2000), 711-727.

[Beu97] F. Beukers and D. Zagier, *lower bounds of heights of points on hypersurface,* Acta Arith. **79** (1997), 103-111.

[Bom02] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$*,* Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei(9) Mat. Appl. **12** (2001), 5-14 (2002).

[Bre51] R. Breusch. *On the distribution of the roots of a polynomial with integer coefficients.* Proc. Amer. Math. Soc. **2** no. 6. (1951) 939-941.

[Bla71] P.E. Blanskby and H.L. Montgomery, *Algebraic integers near the unit circle.* Acta Arith. **18** (1971), 355-369.

[Boy81] D. W. Boyd, *Speculations concerning the range of Mahler's measure,* Canadian Math. Bulletin **24** (1981), 453-469.

[Can82] D.C. Cantor and E.G. Strauss, *On a conjecture of D. H. Lehmer,* Acta Arith. **42** (1982), 96-100:corrigendum, ibid.,327.

[Dre98] G.P. Dresden, *Orbits of algebraic numbers of low heights,* Math. Comp. **67** (1998), 815-820.

[Dob79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial,* Acta Arith. **34** (1979), 391-401.

[Dub05] A. Dubickas and M. Mossinghoff, *Auxillary polynomials for some problems regarding Mahler's measure,* Acta Arithmetica **119.1** (2005), 65-79.

[Dum99] D.S. Dummit and R.M. Foote, *Abstract Algebra, Second Edition.* John Wiley and Sons Inc., 1999.

[Eve99] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics,* Springer-Verlag, 1999.

[Fes02] I.B. Fesenko and S.V. Vostokov, *Local Fields and Their Extensions, Second Edition.* American Mathematical Society, 2002.

[Hoe93] G. Hoehn and N.P.Skoruppa, *Un resultat de Schinzel,* Journal de Th éorie des Nombres de Bordeaux **5** (1993), 185.

[Kob77] N. Koblitz, *P-adic numbers,* Springer-Verlag, 1977.

[Koc00] Helmut Koch, *Number Theory, Algebraic Numbers and Functions.* American Mathematical Society, 2000.

[Kro57] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten,* J. Reine Angew. Math. **53**(1857), 173-175.

[Leh33] D. H. Lehmer, *Factorization of certain cyclotomic functions,* Annals of Math. **34** (1933), 461-479.

[Lou83] R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique,* C. R. Acad. Sci. Paris Sér. I 296 (1983), 707-708.

[Mah60] K. Mahler, *A application of Jensen's formula to polynomials,* Mathematika **7** (1960), 98-100.

[Mah61] K. Mahler, *On the zeros of the derivative of a polynomial,* Proceedings of the Royal Society **264** (1961), 145-154.

[Mah62] K. Mahler, *On some inequalities for polynomials in several variables,* Journal of the London Math. Soc. **37** (1962), 341-344

[Mah64] K. Mahler, *An inequality for the discriminant of a polynomial,* Michigan Math. Journal **11** (1964), 257-262.

[Mig78] M. Mignotte, *Entiers algébriques dont les conjugués sont proches du cercle unité,* Séminaire Delange-Pisot-Poitou, 19e année: 1977/78, Théorie des nombres, Fasc.2, Exp. No. 39, 6 pp., Secrétariat math., Paris, 1978.

[Ost18] A.M. Ostrowski, *Über einige Lösungen der Funktionalgleichung* $\phi(x)\phi(y) = \phi(xy)$. Acta Math. **(41)** (1918), 271-281.

[Rib99] P. Ribenboim, *The Theory of Classical Valuations,* Springer-Verlag, 1999.

[Sam06] *Lower bounds on the pojective heights of algebraic points,* Acta Arith. 125.1 (2006), 41-50.

[Sch73] A. Schinzel, *On the product of the conjugates outside the unit circle of*

an algebraic number, Acta Arith. 24 (1973), 385-399; Addendum, *ibid.* **26** (1973), 329-361.

[Sha54] I.R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR. Ser. Mat. **18** (1954), 525-578.

[Smy71] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. Lond. Math Soc. 3 (1971), 169-175.

[Ste78] C. L. Stewart, *Algebraic integers whose conjugates lie near the unit circle,* Bull. Soc. Math. France **106** (1978), 169-176.

[Val07] J. Vaaler, *Topics in Algebra, Spring 2007,* The University of Texas at Austin.

[Vou96] P. Voutier, *An effective lower bound for the height of algebraic numbers,* Acta Arith. **74** (1996), 81-95.

[Was82] L.C. Washington, *Introduction to cyclotomic fields,* Springer-Verlag, 1982.

[Zag93] D. Zagier, *Algebraic numbers Close to both 0 and 1*, Math. Comp. **61** (1993), 485-491.

[Zha92] S. Zhang, *Positive line bundles on arithmetic surfaces,* Annals of Math. **136** (1992), 569-587.

Vita

John Matthew Garza was born in Brownsville, Texas on December 25, 1975, the son of Reynaldo Garza Jr. and Trudy Clifton. After completing his work as a high school student he enlisted in the United States Navy where he served aboard the U.S.S. Houston. Following the Navy he enrolled in the Texas Southmost College in Brownsville. He was accepted as a transfer student by The University of Texas at Austin the following year and completed a B.S. in Mathematics in August of 2001. He began graduate studies at The University of Texas at Austin in August of 2002.

Permanent address:

317 Creekbend
Brownsville, Texas
78521